CENTRE FOR CRIMINOLOGY
FACULTY OF LAW

MSc Criminology and Criminal Justice 2023-24
Dissertation Submission Cover Sheet

Name:	**Scarlet Rosalie Biedron**
Dissertation Title:	**Cybercrime in the Digital Age: How Big Data, Cryptocurrency, and Communication Networks Shape Cyber Offending, Cyber Security, and Law Enforcement**
Word count:	**14,963**

Abstract

Cybercrime is a global problem impacting the lives of millions every year. Individuals, private companies, government agencies, and nations face the threat of crime perpetrated using computers and/or the internet. The digitization of society and the economy transforms the landscape of our lives. As technology becomes increasingly ubiquitous around the world and increasingly pervasive in people's lives, so too does cybercrime, the impacts of this crime, and the need for cyber security. The analysis looks at how technologies of the digital age affect cybercrime offending, cyber security, and law enforcement. The focus of this work is on the categories of technology that illustrate how technology simultaneously enables cyber offending and cyber policing: big data, cryptocurrency, and communication networks. The study relies on theoretical frameworks from sociology, criminology, and technology, such as Marxist theories of capital production, Routine Activity Theory, and Actor-Network Theory. The investigation is grounded in an examination of key cases including the British Library hack, the Lazarus heist, the TalkTalk hack, the Petya attacks, and the coordinated takedown of AlphaBay and Hansa Market with law enforcement efforts referred to as Operation Bayonet and Operation GraveSac. The analysis contributes to the body of criminological literature with a unique analysis of the role technology plays in cybercrime by combining existing research, a cross-disciplinary theoretical approach, and an in-depth view of criminal and law enforcement cases. It further adds to academic, practical, and policy-oriented approach discussions of the growing field of cybercrime with a critical analysis of offending, policing, and security methods and approaches. However, further research is needed to better understand the continuously evolving environment of cybercrime as well as the cyber police and security efforts mandated by prevalent cybercriminal activity.

Table of Contents

Introduction

On a global scale, the costs of cybercrime are high and pervasive. These costs are not just financial but also social. The problem of cybercrime is immense, ubiquitous, and international. It impacts individuals, communities, private entities and companies, public institutions and agencies, and nations. At the heart of the problem is technology. In our contemporary world, technology, the internet, and digital transactions connect us and allow our societies, economies, and countries to function. As of 2024, about 67% of the world's population uses the internet (Petrosyan, 2024a). However, they also allow for crime to be committed in new ways. Cybercrime is crime committed by means of or using the internet or computers, and technologies such as computers can be the target, tool, or accessory in cybercrimes (Sukhai, 2004). The limitations of traditional street crime to finite location, victim, and scale are completely redefined in the technologically enabled world with cybercrime. As the world becomes increasingly digital, it also becomes increasingly plagued by cybercrime. One of many examples of cybercrimes this year is the cyber-attack on the British Library in October 2023 perpetrated by a ransomware gang called Rhysida (British Library, 2024). Technology creates a novel criminal landscape in cyber space and allows cybercrime to enter and affect people's lives and livelihoods around the globe.

In this dissertation, I investigate the ways in which the technologies of the digital age affect cybercrime. I argue that technology is a catalyst for creating, maintaining, and developing the world of cybercrime. Specifically, I focus on technologies of big data, cryptocurrency, and communication networks. These three categories of technologies exemplify the unique environment of the cyber world as they simultaneously enable the digitally developed world, cyber offending, and cyber enforcement. As such, I discuss them

throughout all three chapters in order to examine the complex interconnected dynamics between and intersection of technology, offending, and law enforcement and security. Placing technology in the centre of the analytical frame, I explore the ways in which the criminological world of cybercrime is unique in regard to the problem(s) it poses to society, cyber offending, and cyber enforcement. In Chapter 1, The Problem: Cybercrime in the Digital Age, I discuss the landscape of cybercrime and its impact on the world, and I provide a brief history of the intertwined development of technology and cybercrime. I then discuss the three categories of technologies which offer apt examples of the intertwined nature of the digital age and cybercrime. Lastly, I apply a Marxist theoretical framework to understand the continued expansion and perpetuation of the digital world and the cybercrime that accompanies that world. In Chapter 2, Cybercrime Offending in the Digital Age, I focus on cybercrime offending. In this chapter, I argue that the technologies of big data, cryptocurrency, and communication networks enable unique forms of offending. I then utilize both criminological and technological theoretical frameworks to understand and derive insights into the relationship between cyber offending and technology. In Chapter 3, Law Enforcement, Security, and Cybercrime, I look at how the same technologies that enable cybercrime offending can also be utilized by law enforcement and cyber security to prevent, detect, and address that crime. Moreover, I discuss how the challenges and problems of cybercrime are addressed by law enforcement. Finally, I use a technologically-centric lens to critically view the current direction and persisting limitations of cyber policing on an international and local level.

Throughout the dissertation, I rely on sources, research, and scholarship from a variety of fields including sociology, criminology, law, and technology. Specifically, I utilize academic articles, books, and empirical research as well as government reports, legal cases, news articles, and documentaries. Moreover, I draw on specific cybercrime cases and law enforcement efforts throughout the proceeding work as key examples. I also apply select criminological, sociological, and technological theoretical perspectives to derive insights into the digital age, the field of cybercrime, and the role of technology in cyber offending and enforcement. These are of course not the only perspectives that can and should be applied to this topic or the only cases that represent valuable examples; however, they offer avenues of investigation, analysis, and exemplars that I find particularly interesting. Although this dissertation looks at the global scale, scope, and nature of the digital world and cybercrime, it is also limited by a relatively Euro-American focus. The limited geographical scope is due in part to the occurrence of cybercrime and enforcement efforts in those places, the focus of the corpus of relevant research that looks at or is produced in North America and Europe, and my own positionality and biased interest as an American student studying in the United Kingdom. In this way, this dissertation is limited by its selective focus and analytical frame, examples, and cases. Although additional exploration is necessary to further explore this topic and rapidly growing field, it is beyond the scope of this work.

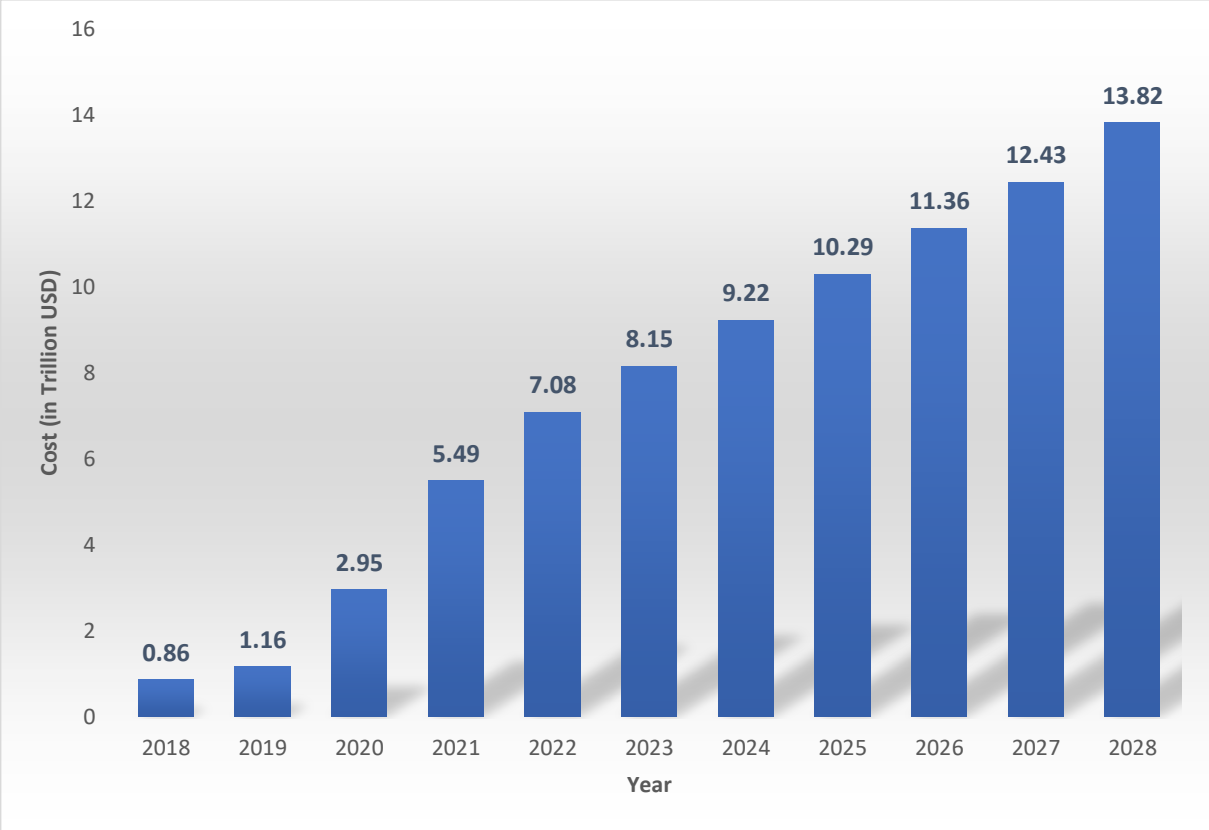
Chapter 1: The Problem: Cybercrime in the Digital Age

To analyse how technologies of the digital age affect cybercrime, it is critical to first understand the problem of cybercrime, the consequences of that problem, and the technology and data-powered cyber world from which that problem emerges and continues. In this chapter, I analyse the problem of cybercrime and argue that technology is the central instrument which creates and perpetuates it. To make this argument, I discuss 1) the contemporary impacts and landscape of cybercrime, 2) a brief recent history of how technology and cybercrime develop in interconnected ways, and 3) the contemporary digital age and how communication networks and devices, cryptocurrency, and the world of big data foster that world and set the stage for cybercrime. Finally, I analyse the current state of the digital world through a Marxist theoretical framework.

The Impacts and Current State of Cybercrime

Cybercrime costs our global society trillions of dollars every year. According to Statista, the annual cost of cybercrime worldwide in 2023 is estimated at 8.15 trillion (USD) (Fleck and Richter, 2024). This is a substantial rise from less than a trillion in 2018, and this increase is predicted to continue and reach 13.82 trillion in 2028, as illustrated by Graph 1 (Fleck and Richter, 2024). According to eSentire data, over the course of this year – 2024 – cybercrime is predicted to cost 9.5 trillion USD (Freeze, 2023).

Graph 1: Estimated Global Costs of Cybercrime[1]

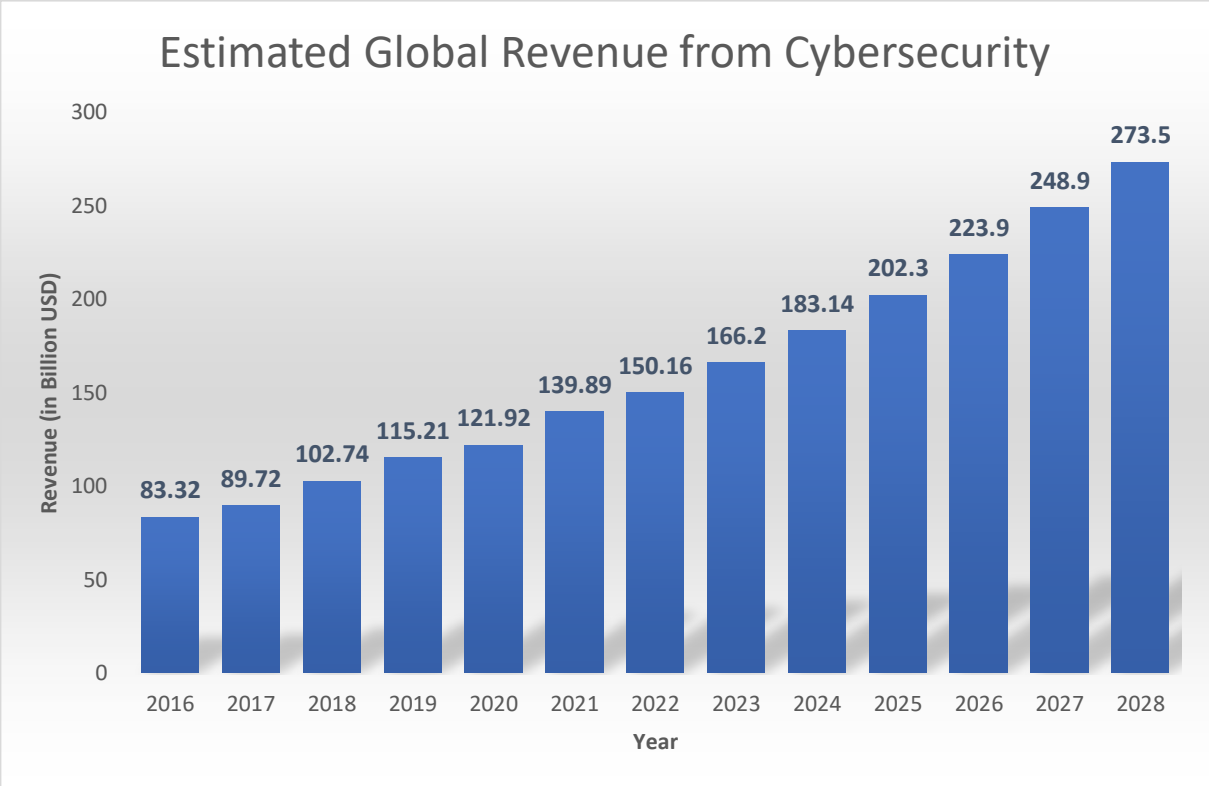


These figures for the cost of cybercrime include destruction of data, financial theft, fraud, embezzlement, stolen intellectual property, lost productivity, etc. (Freeze, 2023). In the United States alone, there are over 3,000 data compromises in 2023, which affect over 350 million individuals (Petrosyanb, 2024). However, they cannot cover the social costs of disruption and damage to individual lives, businesses, and organizations such as those that come along with disrupting the operations of hospital systems responsible for the healthcare, medical needs, and lives of patients.

[1] The Data in this graph are from Data from Statista Market Insights (2023); Fleck, A. and Richter, F. (2024) Cybercrime Expected to Skyrocket in Coming Years, Statista Daily Data. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/.

As cybercrime advances so too does the cyber security industry and law enforcement effort to address it. According to Statista, the data risk and cyber threats drive the cyber security market which experiences substantial growth with global "revenue increasing from US$83.32 billion in 2016 to approximately US$166 billion in 2023", as illustrated by Graph 2 (2023).

Graph 2: Estimated Global Revenue from Cybersecurity[2]



Alongside revenue, cyber security spending continues to increase substantially in recent years. In 2021, the estimates for spending on cyber security technologies reach over 70 billion (Borgeaud, 2023). Looking specifically at organization spending, McKinsey reports that organizations around the world spend about $150 billion on cyber security (Aiyer et al.,

[2] Statista (2023) Cybersecurity - worldwide: Statista market forecast, Statista. https://www.statista.com/outlook/tmo/cybersecurity/worldwide#analyst-opinion.

2021). Likewise, there is also significant government spending and budget allocation to bolster cyber security efforts. The United States is allocating about "$13 billion of budget authority for civilian cybersecurity-related activities" for the 2025 fiscal year (White House, Office of Management and Budget, 170). Although these facts and figures are difficult to comprehend in regard to practical implications as most are estimates and include different data, they help paint a clear picture; cybercrime is a serious problem. The costs of cybercrime are high. The impacts and ripple effects are felt everywhere around the world on economic, social, and individual levels. Within the cyber world, the growth of offending and enforcement efforts are deeply interconnected.

Cybercrime is a broad category which encompasses many different types of computer crime, and there are many different forms and modes of cyber offending. For example, cybercrime can take the form of traditional crimes that occur through or by means of the internet or computers: illegal sale of goods or services such as drugs, weapons, or false documents, fraud, identity theft, digital theft, spreading hate, etc. Some cybercrimes occur on or using forums or digital marketplaces like those on the darknet – a part of the internet which is encrypted, anonymous, not monitored, and only accessible with certain software such as Tor. Tor, an acronym for The Onion Router, is "the encryption software that allows users to visit sites" on the dark web, and its "protocol is a kind of digital invisibility cloak, hiding users and the sites they visit" (Bearman, 2020a, 4). There are also criminal activities that come about through the digital world such as hacking, malware, ransomware, phishing, etc. Malware refers to malicious software and can come in different forms such as a computer virus, worm, trojan horse, spyware, adware, etc. (Loebenberger and Wielputz, 2006). Malware infects software, spreads or replicates itself, sometimes infects other programs, and sometimes

performs secret functions or comes along with effects unintended by the user (Loebenberger and Wielputz, 2006).

Ransomware in particular accounts for the most significant financial costs of crime each year. Ransomware attacks are a form of "data-based extortion" which are often paid off with cryptocurrency such as Bitcoin, discussed further in the following sections (Richardson and North, 2017, 10). Ransomware is essentially "malware that locks your computer or prevents you from accessing your data using private key encryption until you pay a ransom" (Richardson and North, 2017, 10). Ransomware attacks are often perpetrated by hacking groups who are active on darknet forums and sites. Individuals, companies, public agencies, or institutions that are victims of these attacks are unable to access their data when they are encrypted, and the ransomware offenders or hacking groups threaten to release the sensitive data to the public and/or not give the company access if they do not pay. Although there is no guarantee the hackers will do as they say once ransom payment is made, ransomware payments around the world hit a record of over a billion USD in 2023 (Greenberg, 2024). There are two basic types of ransomware: crypto and locker (Richardson and North, 2017). While locker ransomware simply locks the data on a device, crypto ransomware encrypts the data so that even if the malware is removed or storage is moved to another device, the data is inaccessible (Richardson and North, 2017). One such example is the recent Ticketmaster data breach, perpetrated by a hacker group called ShinyHunters in May 2024, which compromised the personal and credit card details of over 500 million customers (Deb, 2024; Gecsoyler, 2024). ShinyHunters' recent ransom demand for the 1.3 terabytes of data is $500,000 USD (Deb, 2024). The threat of ransomware attacks and data breaches constantly loams in the

digital age. Cybercrime offending and the ways in which it is enabled by technology are discussed in greater depth in Chapter 2.

Brief History of the Cyber World

The modern world of cybercrime is enabled by technology. Malware, computer crimes, and illegal online activity are made possible by the advent, development, and maintenance of the digital environment which are necessitated by the very definition of cybercrime. The interconnected nature of technology and computer crime as well as its creation of and proceeding effect on cybercrime is evident in the parallel, conjoined development of the two in recent history. Crime on, by, or through computers and the internet is not the afterthought of criminals looking to scale or grow their criminal enterprises. The advent and development of antisocial or illicit activities, tools, and technology (e.g., malware, hacking, etc.) not only occurs in parallel with the advent and development of the intended, conforming activities, tools, technologies themselves (e.g., the internet, computers, etc.) but also propels the advancement of those licit technologies forward. Put another way, both the use and misuse of technology are equally central for development of the digital world. What we call cybercrime today is critical to the creation of everything cyber. In the digital world, progress is progress – legal or not. Because of this, I use a technological lens to make this cyber-crime relationship visible in the following outline and evaluation of the brief history and the modern landscape of cybercrime.

The progression of cybercrime coincides and is made possible by the technological revolution. In 1969 the ARPANET, the world's first computer network and the precursor to the internet, is first used - mainly for the scientific and academic research community

(Abbate, 1999; Leiner, 1997). In 1971, the first computer virus, the Creeper Virus – technically a computer worm –, appears on ARPANET (Loebenberger and Wielputz, 2006). Creeper essentially functions to replicate itself on computers across ARPANET and display a message, "I'm the Creeper: catch me if you can" on each infected device (Loebenberger and Wielputz, 2006). Developed by Bob Thomas to test his theory about moving across the network, Creeper is relatively benign and stopped by the anonymously released antivirus, Reaper (Loebenberger and Wielputz, 2006). The first malware reflects an instance of technological development with negative consequences (perhaps unintended or perhaps unforeseen in their effect). Throughout the history of the cyber world, technological innovation and research frequently account for the intent behind developments in cybercrime techniques and methods.

The pattern of technological experiments gone wrong continues throughout the rest of the 20th century. In 1983, there is a switch to TCP/IP network protocol from which the modern internet grew (Leiner, 1997). By 1985, email is used more widely (Leiner, 1997). Then, in 1988, the first email worm, called Morris Worm, inflects systems all over the internet, "caus[ing] an estimated damage of $96,000,000 by highly increasing the global network" traffic despite the seemly innocuous intention of its creator to "gauge the size of the internet" (Loebenberger and Wielputz, 2006, 4; Spafford, 1989). The repercussions of this lead to the first Computer Emergency Response Team (CERT), a milestone in addressing the problem of early forms of cyber 'crime' (Spafford, 1989). In the 90s, DOS/Windows computer systems dominate the market along with the growing popularity of the World Wide Web (WWW) (Loebenberger and Wielputz, 2006, 5). These technological advancements too are simultaneously plagued and advanced by viruses and malware. For example, the

Chameleon virus (1990) reflects research development seeking to demonstrate novel abilities with encryption and detection avoidance (Loebenberger and Wielputz, 2006).

The technology-cybercrime relationship gives rise to an additional focus in technological innovation: security. In a world where new technology allows for exponential advancements in almost every aspect of human life and productivity, what is to be done about the negative impacts that come along with such cutting-edge progress? The '90s reflects a time when technological innovation expands to include a security focus in the face of digital insecurity. In 1994, the first secure online transaction sets the foundation for a future of ecommerce (Schwartz, 1997). Throughout the '90s, electronic commerce becomes a prominent topic for businesses, the law, and addressing new forms of cybercrime (e.g., fraud, hacking, etc.) that accompany it; as such, security measures to address cybercrime expand with cryptography, electronic signatures, etc. (Austin, 1999). What emerges by the end of the 20th century is a pattern of technological innovation that is inexplicably intertwined with forms of 'malicious' cyber activity and cybercrime. The positive developments of the digital era and the negative consequences critically coproduce each other as they both further progress. The problems of cybercrime propel the solutions. Part of these solutions includes the formation and expansion of responses to cybercrime: antiviruses, security, detection software, regulations, law, and enforcement.

This pattern continues in the 21st century. As the technological revolution re-centres the lives of millions to include, depend on, or revolve around technology, the social, economic, and political spheres of society interact with and react to these patterns. The scale of technological innovation mushrooms in the early 2000s, and the influences and impacts of activity in the cyber world now have the potential to affect the daily lives of millions in

critical ways. The implications are no longer limited to those interested in tech; the functioning of businesses, economies, cities, and nations are at stake. The scale is global. The actions of one (whether well intended or not) have the potential to impact us all. The nature of a world connected by a network that operates almost instantaneously is that the technology that empowers that network or operates on it gains a certain agency that exceeds its individual creator and that creator's intent. In 2000, the infamous ILOVEYOU virus affects millions with estimated damage of $5.5 billion (Loebenberger and Wielputz, 2006). In November of 2000, the United Nations General Assembly adopts the United Nations Convention against Transnational Organized Crime. In Article 29.1, the convention describes that party states shall initiate law enforcement training programs, which deal with, in part, "methods used in combating transnational organized crime committed through the use of computers, telecommunications networks or other forms of modern technology" (UN Convention against Transnational Organized Crime, 2000, 31). Although the UN Convention is not directed specifically toward addressing cybercrime, it is significant as a milestone whereby the problem of digital or computer-enabled crime is recognized and the need for legal and law enforcement response is raised to the stage of international criminal justice. Following this, in 2001 the Budapest Convention on Cybercrime sets out to pursue "a common criminal policy aimed at protecting society against cybercrime" (The Budapest Convention, 2001, 1).

In 2005, Trojan Gpcoder (also known as GP Code), the first modern ransomware, is released (Richardson and North, 2017). In 2008, Satoshi Nakamoto publishes his Bitcoin whitepaper on blockchain technology and cryptocurrency (Nakamoto, 2008). This milestone reflects a turning point in the digital era toward cryptocurrency which enables

ransomware to take off with large-scale attacks by 2011. An online blackmarket, called the Silk Road, which uses Bitcoin, emerges on the dark web in 2011 and is taken down by the FBI in 2013 (Bearman, 2020ab). By 2012, there are toolkits being sold on online forums and marketplaces, such as one called Citadel, priced at $3,000, which enable ransomware, making it simple to create and distribute (Richardson and North, 2017). The infamous CryptoLocker ransomware is first released in 2013 and infects hundreds of thousands of victims with the FBI estimating $27 million ransom pay outs by the end of 2015 (Richardson and North, 2017). In 2014, the distribution servers for CryptoLocker are taken down by a group of law enforcement agencies, researchers, and security vendors (Richardson and North, 2017). Other forms of improved, deceptive ransomware, such as CryptoWall, CTB-Locker, and TorrentLocker, continue to emerge in the following years (Richardson and North, 2017). In 2017, the WannaCry ransomware attack infects more than 300,000 computers in 150 countries (Chappell and Neuman, 2017). The White House at the time publicly blames North Korea, which reflects the risk of cyberwarfare and state-sponsored attacks (Chappell and Neuman, 2017). The 2020 SolarWind hacks (Temple-Raston, 2021) and the 2021 Colonial Pipeline attack (Easterly and Fanning, 2023) further reveal the potential for and attention to state-sponsored cyber-attacks, the vulnerability of US agencies, infrastructure, and supply chain, and the status of cybercrime on the international stage. As technology ushers the world into the productive and advanced futuristic 21st century, it also gives way to unprecedented forms of crime. Inherent in the developments of software and the cyber world more broadly, are malware and cybercrime.

Technological Foundations of Contemporary Cybercrime

In the contemporary digital era, there are three categories of technology that significantly contribute to the structuring and functioning of the cyber world. These categories involve many specific technologies with numerous, multifaceted, interconnected aspects but it is conceptually useful to discuss them consecutively. The ways in which all three enable and impact both cyber offending and cyber enforcement are discussed in Chapter 2 and Chapter 3 respectively. The first is communication networks and devices. Technology for communication such as the internet, social media, mobile communication, and smartphones connect the world within and across borders. The internet connects about 5.44 billion users, or 67% of the global population, and social media connects about 5.07 billion, or about 62% of the global population (Petrosyan, 2024a). According to the World Economic Forum, "5.4 billion people worldwide have at least one mobile subscription" (Richter, 2023), and over half of the global population, about 54% or about 4.3 billion people, own a smartphone as of 2023 (Shanahan and Bahia, 2023). Technology facilitates a global network of communication and connection which empowers human activity, industry, and our sociopolitical and economic world at large. However, communication mechanisms and devices of the digital age also create avenues for cybercrime as both tools for committing offences and targets for crimes (see Chapter 2 for further detail).

The second is cryptocurrency and the digital economy. Across the world, technology increasingly acts as a conduit for how people access and engage in the economy. According to the World Bank, the share of account owners using digital payments in developing economies is 57% as of 2021, up from 35% in 2014, and the share of account owners using digital payment in high-income economies is 95% as of 2021, up from 88% in 2014 (Demirgüç-Kunt

et al., 2022). There are three specific technologies that exemplify the ways in which the online economy is a critical component of both the productive digital world and the cybercrime world: 1) online marketplaces, 2) digital and mobile banking, and 3) cryptocurrency. The 'dark' side of these technologies as enablers of cybercrime is discussed in greater detail in Chapter 2. Online marketplaces are forums for globalized commerce and push forward our interconnected international world for individuals as well as businesses. For example, digital marketplaces like Facebook, Amazon, eBay, and Etsy facilitate third-party sellers, which allow business and individuals to sell their products and services online through widely used platforms. The modern marketplace is online. About 17% of all business-to-business transactions and about 47% of digital consumer purchases around the world are estimated to occur through online marketplaces and e-commerce (Meteor Space, 2023). The technology of the digital age not only facilitates online marketplaces but also online banking. Banking is increasingly digital, online, and mobile. Not only does this improve well-developed economies but also developing economies as technology for online or mobile banking fosters greater access to the economy for people and communities around the world (Demirgüç-Kunt et al., 2022). Over half the world's population own a smartphone, according to a GSMA 2023 report (Shanahan and Bahia, 2023). In Sub-Saharan Africa, about 33% of adults have mobile money accounts, making "mobile money… an important enabler of financial inclusion in Sub-Saharan Africa—especially for women—as a driver of account ownership and of account usage through mobile payments, saving, and borrowing" (Demirgüç-Kunt et al., 2022, 2).

Lastly, the digital economy includes cryptocurrency which is a form of digital currency that is decentralized and not controlled or regulated by centralized financial institutions. There are thousands of cryptocurrencies such as Bitcoin, Ethereum, Solana, and

Cardano (Hicks and Adams, 2024). Cryptocurrency is a term usually used to refer to crypto 'coins' that run on their own blockchain, but there are also crypto 'tokens' which represent digital assets or utilities stored on the blockchain database (Hicks and Adams, 2024). On the Ethereum blockchain, for example, "different tokens represent different values, whereas Bitcoin is valued in straight US dollar terms" (Minnaar and Reddy, 2018, 71). Given that Bitcoin is the most popular and widely used form of cryptocurrency, it is helpful to focus specifically on it for the purposes of understanding how it works and its benefits. As previously noted, Nakamoto's (2008) landmark whitepaper proposes direct transactions through a "peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions" which allows payment systems to rely on cryptographic proof instead of trust of third parties (e.g., centralized banking systems) (Nakamoto, 2008, 1). A cryptocurrency is created by a computational process called 'mining' whereby "cryptographic algorithms" are used to "protect the integrity of [Bitcoin] transactions" (Minnaar and Reddy, 2018, 74). Transactions are stored with blockchain technology on a digital ledger which essentially irreversibly, transparently, and chronologically tracks all of the activity (Minnaar and Reddy, 2018). For those, like me, who are not well versed in computer science or software engineering, think of a dollar that has a ledger of previous transactions on it, but this dollar is digital. There are many benefits to cryptocurrencies such as a lower risk of inflation, efficient transactions, minimal to no transaction costs, and transparency while also being private (Tambe and Jain, 2024). Because of blockchain technology, transactions are transparent and can be tracked; however, they are also private with pseudonym identifiers such that they don't contain any personal information (Tambe and Jain, 2024). Bitcoin and cryptocurrencies are helpful for preventing fraud or falsified

transactions. Yet, they are also decentralized and anonymous making them apt for illegal online commerce, criminal transactions, and ransomware (see Chapter 2).

The third category of technology is big data. In the digital age, our world and our lives are monitored through the technology we rely on to function in our day-to-day reality. The digital revolution and technological revolution exist as a result of the collection and analysis of data (Saha, 2021). In a Forbes article, Saha notes that the "IDC calculates that in 2010 the world created about two zettabytes (ZB) of digital information which is the equivalent of enough 1 BG thumb drives, placed end to end, to stretch the length of 184 million football fields" (2021, 1). The IDC further predicts that the global 'datasphere', as they call it, to grow from 33 zettabytes in 2018 to 175 zettabytes by 2025 (Rydning et al., 2018). All of that is to say we are a global society driven by data and a lot of it – an almost unfathomable amount. Big data, data storage, and data-powered technology do not only offer the foundation that propels forward innovative manufacturing of valuable products, it empowers and informs the cyber world. Communication devices and networks connect our world and allow our actions and interactions to be translated into the language of data. The fact that data are valuable makes them worth holding for ransom, stealing, or hacking. And cryptocurrency makes those digital crimes profitable.

A Theoretical Framework of Digitization

The digital world, the technologies that enable that world, and the cybercrime that accompanies it can be understood through a Marxist theoretical framework. The monitoring and monetization of the consumer in the capitalist world turns data into capital. The process of digitization continues and reproduces itself because of the capitalist value that is placed on

data and technology. This is, of course, not the only theoretical avenue to conceptualize the digital age; however, this approach offers a useful perspective to understand the intersection of technology and the cyber world which sets the foundation for the proceeding chapters. Similar to the analogy of knowledge production to capital production, outlined by Comaroff and Comaroff (2015), an analogy of data production to capital production is evident with this theoretical framework. Individuals and human activity are surveilled and their data are collected much like natural resources are mined. Almost every facet of our existence as consumers is documented as data and then monetized. AI and the Internet of Things (IoT) – technologies that communicate with one other such as 'smart' devices – allow technology to simultaneously act as useful convenient tools for everyday life as well as surveillance systems which collect data (Wall, 2018). Once collected, these data are produced into knowledge, insights, and something useful and of value much like the way materials are manufactured in products. Finally, the value produced by this data is utilized to sell products and services back to individuals in more customized, personalized offerings that make them more appealing to the individual consumer. This is evident with personalized ads which display more consumer-centric product offerings and predictive and anticipatory shipping which allows the products consumers have yet to buy to be in warehouses in their geographic region prior to purchase. From everything like large language models (think AI and ChatGPT) to ad recommendations (think cookies and Google), data enable business, technology, and the economy. The cycle of value production through digitization sets the foundation for understanding the self-perpetuating nature of the digital age.

Several scholars apply capital and colonial lenses to analyse the data economy (e.g., Couldry and Mejias, 2019; Sadowski, 2019; Ström, 2022; Thatcher et al., 2016). Using a

Marxist framework and building on Bourdieu's (1986) forms of capital, Sadowski argues that rather than treat data as a commodity, data should be viewed as capital (2019). In this way, "datafication takes shape as a political economic regime driven by the logic of perpetual (data) capital accumulation and circulation" (Sadowski, 2019, 2). Unlike the value of many physical materials, data scarcity does not inversely correlate with value. In the realm of big data, the more data you have, the more useful it is as the insights, predictions, and calculations become more accurate and generalizable. Therefore, the process of digitalization is exponential because the monitoring and collection of data and the monetary gains of data as a form of capital are infinite. When analysed through this framework, digitization is an odd form of value production whereby the behaviour of a consumer is documented, made valuable, and used to bolster profit. Yet, this process occurs without the individual consumer – the source of the data – seeing any realized monetary gains for their 'raw materials'. Our data are not subject to the intellectual property or patent laws that ideas, inventions, or labour are. Data form their own capitalist category. Therefore, as Couldry and Mejias (2019) and Thatcher et al. (2016) argue, the contemporary economy of big data operates through 'data capitalism' and 'data colonialism' whereby data dispossession and appropriation are seen as natural, desirable processes of "digital frontierism" (Thatcher et al., 2016, 992). Part of the process of data colonialism is the accumulation of capital which occurs through an "asymmetric power relationship in which individuals are dispossessed of the data they generate in their day-to-day lives" (Thatcher et al., 2016, 990). The intrusive nature of digital surveillance and data colonialism are concealed by the conduit of technology. The framework set out by scholars, which views data as capital in a digital political economy of power, creates a helpful perspective on data. Made evident through this framework are the ways in

which data are given value and drive innovation, development, and progress in the digital economy.

This digital framework and analytical foundational are helpful in understanding the drivers that maintain and produce the unique dynamics and reality of the cyber world and crime that accompanies it. The cybercrime world is more complicated, multifaceted, and evolving than the world of traditional street crime. More traditional forms of crime, especially those predating the internet, operate along a linear relationship between offenders and enforcement. The things that benefit criminal offenders make the job of law enforcement officers and police more difficult and vice versa. Developments and innovation are either uniquely pro-offending or uniquely pro-enforcement. It is an adversarial, zero-sum game. The traditional offender-enforcement engagement typically involves a constant balancing of mutually exclusive scales; cops versus robbers constantly leveeing for the upper hand. The technological revolution changed all of this. In the digital age where interactions are online, communication is global, data is in demand, and currency is crypto, technological innovations enable offending at the same time as they enable law enforcement efforts to address, detect, and prevent that offending. The relationship is no longer a binary, linear battle but instead a complex and intertwined dynamic. This complex offending-enforcement relationship is exemplified by the technologies within the categories of communication networks, cryptocurrency, and big data. It is part of what makes the world of cybercrime unique. It is critical for the understanding, analysis, and research of cybercrime as well as the ways in which that research can be transformed into and inform pragmatic action to address the global problem of cybercrime. The proceeding chapters analyse the ways in which the technologies

of the digital era affect cybercrime in regard to offending, law enforcement, and the unique relationship between the two.

Chapter 2: Cybercrime Offending in the Digital Age

As technology advances, it propels and affects cybercrime and methods of offending. The inverse is also true, methods for cybercrime often necessitate and advance technological development. This is not to say that instances of innovation in cybercrime or technology always reflect good intentions or do not sometimes reflect malicious intent. Cybercriminals can be inventive. However, there is an inherent connection between 'productive' and 'counterproductive', software and malware, within the technological developments that occur in the digital age. This connection creates an unusual landscape for cybercrime and the ways in which it's changed by technological advancements. In this chapter, I explore the connections between technology and cybercrime in regard to offending. I argue that technology of the digital age is a catalyst for progress at the same time as it enables offending. By bringing technology to the analytical centre, the same benefits of technology (detailed in Chapter 1) can be understood to also form a unique criminological environment with cyber offending that is accessible, anonymous, and scalable. First, I analyse the role of big data by describing how the cycle of digitization and big data technologies facilitate digital offending. Second, I explore the online economy by discussing the dual nature of online marketplaces, digital and mobile banking, and cryptocurrency. Third, I describe the ways in which online and mobile communication creates novel avenues and targets for cyber offending. Finally, I apply theoretical perspectives from both criminology and technology

fields to derive insights about cybercrime offending, technology, and how their complex relationship creates a unique cyber world.

Big Data and Cybercrime Offending

A procyclical relationship exists between big data and cyber offending. This cycle has four parts: 1) data as a resource, 2) technological development, 3) cyber offending, and 4) prioritization of security and enforcement. The first part of the cycle is data as a raw material of monetary value. As discussed in Chapter 1, data are a highly valued resource which are essentially mined and made into something of value. This value drives digitization and technological development which leads us to the second part of the cycle: the technology that is created for and by big data. As a result of the value of data, technologies to facilitate this process and perpetuate it are produced. The data storage industry is a growing and according to Fortune Market Insights, the 2023 global data storage market size is valued at over $185 billion (2024). The accumulation of data on a global scale allows for technology such as cloud computing, automation, data analytics, and generative AI (artificial intelligence) with LLMs (large language models) which have captured the world's attention. As a result of big data, the digital world is faster, more efficient, more convenient, and more profitable than ever. Yet, at the same time as big data makes the daily life of law-abiding citizens and businesses more productive and efficient, it also enables illegal activities.

This brings us to the third part of the cycle: cybercrime offending. As Wall describes, the demand for data transforms online and computer-enabled crime such that the shift to big data is accompanied by a shift to "big crime" (2018, 29). Wall categorises these cybercrimes into two types: upstream and downstream crimes. Upstream crimes include data breaches,

distributed denial of services attacks (DDoS), mass spam attacks, ransomware attacks, etc. which cause damage as well as create opportunities for downstream crime (Wall, 2018). Downstream crimes occur "when the stolen data is sold to unscrupulous types who may try to use it to exploit or extort either the individual whose personal information [is] comprised or the owner of the database" (Wall, 2018, 29). The downstream ripple effects can include "disruption of services and business, fraud, scams, hate speech, political interference," and "even cyberterrorism and cyber warfare" (Wall, 2018, 29-30). Upstream, the value of data makes it a target for cybercrime such as ransomware, and the cascading crimes downstream further damage, disrupt, and negatively impact individuals, businesses, organizations, and nations (Wall, 2018). The connection between big data and cyber offending is made evident with examples such as cloud computing, which simultaneously enables the productive cyber world as well as the criminal cyber world. As Wall aptly states, "big data and big crimes are powered by cloud technologies" (2018, 30).

Cloud computing technologies and services refer to data storage, computer power, platforms, etc. that are available over the internet through the infrastructure of data centres. The cloud is critical for most of today's online activity and internet services as "they allow data to be stored and accessed via the internet instead of the user's own hard drive" (Wall, 2018, 30). The proposition of data centres and the cloud for criminals is access to large-scale amounts of data. Data breaches and ransomware attacks occur on a large scale around the globe affecting individuals, companies, and state agencies. For example, a 2023 global cyber-attack exploits a vulnerability in a widely used file transfer software called MOVEit resulting in massive data breaches from the MOVEit cloud (Lyngaas, 2023). The attack, perpetrated by a Russian-affiliated ransomware group / cyber gang called CLOP, has widespread effects on

US government agencies, universities, and hospitals including the US Department of Energy, Shell, British Airways, and Johns Hopkins University.

Online research and academic data centres are often also targeted by ransomware groups who exploit the digital infrastructure, comprise and ransom valuable data, and/or sell or release those data on the darknet. An example of this is the British Library cyber-attack and subsequent 600,000-pound ransom demand (see: British Library, 2024 for the full report; Moules, 2024). The attack, which began in October, 2023, is a result of unauthorized access, through compromised privileged account credentials (login details), to the Library's servers by the hacker group, called Rhysida (British Library, 2024). The expanse of the British Library's remote infrastructure and digital database following the pandemic allow for greater technologically enabled features, development, and online use, but without also implementing additional cyber security measures, such as Multi-Factor Authentication, these developments put the library's system at greater risk for cybercrime (British Library, 2024). The impacts of this attack are pervasive, affecting users and researchers who depend on the British Library, compromising its network, functioning, and about 600GB of files (about half a million documents), including sensitive and confidential information of employees and users (Moules, 2024; Sherwood, 2024). Following the attack, downstream cybercrimes occur such as the sale of the stolen data on the darknet (Sherwood, 2024). The hack is estimated to cost the British Library six to seven million pounds to restore and recover from the damage (Moules, 2024; Sherwood, 2024). The ransomware attack on the British Library exemplifies the widespread impacts, costly damage, and downstream crime that is common with ransomware attacks that target data-rich digital databases of organizations and companies.

The data storage capabilities and data-driven technologies that propel us into the digital future also propel us into a criminal future creating a multitude of constantly evolving methods, tools, and targets for offending. In this way, there is a dark side to big data. As a result, digital security becomes very valuable, and this brings us to the fourth part of the cycle: security and enforcement. When data becomes a target of crime and simultaneously a weapon for crime, the value of security increases. Technological innovation to protect, detect, and prevent crime is incentivised. Further value is placed on these data and the technologies of big data as a result of cybercrime. Thus, the cycle repeats and is self-perpetuating: the increasing value of data capital and the digital economy creates technological growth and development, which in turn enable cyber offending and create a need for security. The connection to security and law enforcement is discussed further in Chapter 3.

Digital Economy and Cybercrime Offending

In the 21st century, the majority of the global economy conducts transactions and banking practices online. As discussed in Chapter 1, technology for digital communication, the internet, and online forums facilitate a globalized, efficient economy which is accessible to almost anyone connected to the internet around the world. However, just as with big data, there is a dark side to e-commerce. As the digital economy develops, so does cybercrime as online transactions are a criminal target, darknet forums enable illegal buying and selling, and cryptocurrency facilitates illegal transactions. The same technologies that propel the productive, legal digital economy simultaneously empower the fraudulent, illegal digital criminal economy. The pattern of technology as a positive force in the world as well as a weapon for criminal activity is evident through the technologies of online marketplaces,

digital and mobile banking, and cryptocurrency. For both criminal and law-abiding individuals, these technologies enable more efficient, simpler, and more anonymous activities, transactions, and communication across and within borders. While the contribution of the technologies of the digital economy are evident in Chapter 1, the ways in which they are also targets and tools for novel and often innovative forms of cybercrime are explored in this section.

The first example of cybercrime in the digital economy is online marketplaces. Illegal transactions occur online every day through forums and marketplaces on the darknet. The darknet (or dark web) "is a corpus of websites that are not visible to the public, but the Internet Protocol (IP) addresses are veiled with anonymity through software tools designed to anonymise the IP addresses" (Minnaar and Reddy, 2018, 74-75). As previously discussed in Chapter 1, The Onion Router (TOR) is the most prominent software for this. Guns, drugs, fraudulent identification and documents, malware, sex trafficking, pornography, illegally obtained data, and pirated media are among some of the products and services that are bought and sold on these forums and marketplaces. They are also filled with discussion threads about everything from gaming to how to hack to conspiracy theories to politics. Infamous marketplaces include the Silk Road, Alphabay, Hansa, and Carder Planet which are all no longer active after enforcement takedowns or shutdowns (Searchlight Cyber, 2023). In 2023, the prominent forums include Exploit, BreachForums, XSS, and RAMP which generally cater to Russian and English speakers (Searchlight Cyber, 2023). Darknet forums play a significant role in the social ties that develop in the world of cybercrime as well as the criminal networks and organizations that allow for the perpetration of crime (Leukfeldt et al., 2017). Online forums essentially act as 'offender convergence settings' where individuals establish social

ties, connect, exchange information and (cyber) tools, engage in commerce, and plan and orchestrate crimes (Leukfeldt et al., 2017).

The second example of the connection between the digital economy and cyber offending is online and mobile banking. As these technologies become ubiquitous (see Chapter 1), so too does cybercrime. Committing financial crimes over the internet, with technological weaponary, is more anonymous, scalable, and less risky than traditional robbery, theft, and fraud. Moreover, cyber offending can be committed remotely and across borders. As technology enables economic transactions to occur digitally, the method of bank robberies also transitions online. The 2016 Lazarus heist is an example of a massive bank robbery perpetrated by a North Korean hacker group known as Lazarus on the Bangladesh Bank. (see BBC News, 2021; Billion Dollar Heist, 2023). Although the transfers stop at $81 million due to a false red flag raised because of coincidence in street names on the paperwork, it is luck (or lack thereof for the hackers) that prevented Lazarus from walking away with their intended $1 billion (BBC News, 2021; Billion Dollar Heist, 2023). A hack of this calibre requires years of planning; it starts with unnoticeable entry into the Bangladesh Bank network through a phishing email sent to employees of the bank (Billion Dollar Heist, 2023). Once in the digital network, the hackers secretly gain access to the secure parts of the bank's computer infrastructure (Billion Dollar Heist, 2023). At the perfectly timed moment, a long weekend that falls on Chinese New Year, the hackers send counterfeit payment orders through the online global system, Swift, which is approved by the NY Fed, sending money to a bank in the Philippines (Billion Dollar Heist, 2023). Once there, a contact at the bank withdrawals the money in cash, and it is then laundered through casinos in Manila (BBC News, 2021). Although some of the money is eventually recovered by law enforcement, millions are

smuggled back to North Korea via private planes (BBC News, 2021). The Lazarus cyber heist is an example of how online banking fosters a globalized, digitized economy at the same time as it puts banking systems at greater risk of cyber-attacks. The technology that allows banking to be more accessible, more efficient, more scalable, and occur remotely on an international scale also allows cybercrimes targeting it to be more accessible, more efficient, more scalable, and occur remotely across borders.

Yet, not all cybercrimes are big scores from a single target like the Lazarus heist. In fact, most take advantage of the fact that a million one-dollar crimes are less risky than a single million-dollar crime (Wall, 2018). Most major cyber-attacks, hacks, and data breaches take advantage of software vulnerabilities to target a multitude of victims to exploit data for ransom or resale. These cybercriminal transactions mainly occur with cryptocurrency – the third key connection between cyber offending and the digital economy. Crypto is the primary currency for criminal transactions. According to a study of illegal activity and cryptocurrency financing, an estimate of 76 billion dollars of criminal activity uses Bitcoin each year which accounts for almost half of all Bitcoin transactions (Foley et al., 2019). That characteristics of cryptocurrency (see Chapter 1) make it the ideal currency for criminals. There is no regulation, oversight, or monitoring which could otherwise flag or prevent transactions. It allows for international transactions in ways previously not possible because the currency is not tied to a state or nation. It creates a level of transparency and reliability while allowing for anonymity through blockchain technology. As Minnaar and Reddy put it, “the dark web and cryptocurrencies make up the ideal formula for quick, anonymous, and relatively easy laundering of proceeds from illegal services and sales” (2018, 74). Because of this, cryptocurrency is used for a multitude of different cybercrimes; for example, it is utilized to

conduct illegal transactions, it is the primary form of payment demanded by hackers for ransomware attacks, it is the centre of frauds, scams, and Ponzi schemes, and it is the target hacking (Minnaar and Reddy, 2018).

In the case of ransomware, hackers and hacker groups seek ransom payments in crypto, often in Bitcoin. An example of this is the 2017 Petya attacks on Ukraine which substantially affected organizations in Ukraine from healthcare to television channels to the radiation monitoring system for Chernobyl (Wakefield, 2017). As with many ransomware attacks, the hackers demand payment in bitcoin in order for victims to recover data. Yet, in this case, it is suspected that the intent of the attackers, speculated to be a Russian hacker group called Sandworm, reflects the desire to cause disruption, mainly to Ukraine – victim to 80% of the attacks (Greenberg, 2018; Wakefield, 2017). Furthermore, cryptocurrency can be a target for hackers who try and gain access to crypto exchange sites or to the 'private keys' of 'virtual wallets' where people's bitcoin is stored (Minnaar and Reddy, 2018). When cryptocurrency is the target of cybercrime, it is essentially a form of online theft through hacking. Examples of this type of cybercrime are often hacked bitcoin exchanges such as Butstamp in 2015 with 19,000 bitcoins (about $5 million dollar's worth) stolen and Bitfinex in 2016 with 120,000 bitcoins (about $72 million dollar's worth) stolen (Minnaar and Reddy, 2018). In this way, the technology of cryptocurrency and blockchain is at the centre of shaping cybercrime as the primary criminal currency, an enabler of cybercrime offending, and a potential target for hacking.

Digital Networks, Mobile Communication, and Cybercrime Offending

As noted in Chapter 1, our world is connected by communication networks, devices, and the internet. However, these technologies are also tools and targets for cybercrime. Phones, mobile devices, and networks are targets for hacking, phishing, and fraud. In a study review of current research, Safavi and colleagues find that the majority of mobile device data breaches result from device loss, theft, or phishing attacks (2013). Phishing attacks are a common entry point for hackers, especially targeting individuals or individual devices, as they disguise malware in email, messages, and other forms of communication as nonthreatening and often attractive messages which entice potential victims to click on them; unbeknown to the victim, this gives hackers access to their devices, accounts, or target. Furthermore, attackers obtain access to mobile devices through malware from downloaded applications, corrupted web-based downloads, or local Bluetooth or Wi-Fi networks (Vashisht et al., 2016). In this way, the technology of mobile devices and smartphones, which is an integral part of the lives of many individuals across the globe, is a potential target for cybercrime; as these devices become more ubiquitous so too does the threat of cybercrime to users.

In addition to the physical devices themselves, mobile networks and services are a target for cybercrime. The TalkTalk hack is an example Distributed Denial of Service (DDoS) ransomware attack occurring in 2015 (Porcedda and Wall, 2019). Hackers exploit vulnerabilities in old but active web pages, and using the SQL injection method, insert malware (Porcedda and Wall, 2019). The attack allows hackers to access TalkTalk's sensitive customer data including their name, address, date of birth, email, telephone number, credit card and bank details (Cellan-Jones, 2015). The TalkTalk hack is an example of how mobile network service providers are a single source to access the data of thousands, in this case, the

compromising the data 156,959 customers with damage estimated at 77 million pounds (Porcedda and Wall, 2019). In this way, even if individual devices are protected and individual activity is secure, the users of mobile services are still at risk because their data is held by mobile network providers, and when they are compromised, personal data can be used to defraud or extort users. Often, following ransomware attacks, not only does a ransomware demand come in from hackers, but the data is often further sold, traded, or exploited (Porcedda and Wall, 2019). This type of cybercrime reveals the potential for downstream and cascading effects that occur with these types of large data breaches and ransomware attacks (Porcedda and Wall, 2019).

Theoretical Perspectives on the Technology-Cybercrime Intersection

The more pervasive technology becomes in our lives and the more ubiquitous it becomes around the world, the more extensive and widespread the impact of cybercrime becomes. Across the spheres of big data, the digital economy and cryptocurrency, and mobile networks and communication, technology acts as a catalyst and target for cybercrime. By applying Routine Activity Theory (Felsen and Cohen, 1979), the self-perpetuating cycle of growth of the technology-cybercrime relationship can be understood as a result of increased opportunity with more offenders, targets/victims, and less police presence. Routine Activity Theory posits that crime increases as a result of circumstances of "likely offenders, suitable target, the absence of capable guardians" (Felsen and Cohen, 1979, 588). In this way, it can be applied to understand the increase in cybercrime as a result of an opportunity that is created through the cyber world with, for example, the increasing amount of valuable data or growing number of mobile network users expanding the suitable targets. Moreover, the

environment of the cyber world lacks visible ‘guardians’ or police and law enforcement agents, and as a result, whether factually accurate, the perception is an absence of capable guardians. Using a Routine Activity approach, the internet, big data, and cryptocurrency can be understood to create a criminogenic environment which enables cybercrime.

Although a Routine Activity approach is compelling, the procyclical and complex nature of the technology-cybercrime relationship calls into question the drivers and consequences of such a relationship. At first glance, this relationship is driven by individual agency in the face of opportunity: people innovate and invent technology which cascades and affects the cyber world by creating greater opportunities for cybercrime. It conceives of victims as suitable targets who engage in risky behaviour (Wagen and Pieters, 2020). Yet, this is not always the case as is evident with large data breaches and ransomware attacks, such as the TalkTalk hack, where victimization of users occurs through the intermediary of a service provider that is hacked creating downstream victimization for users through no fault or risk of their own. Moreover, the significant role of technology is limited to a facilitator of opportunity or potential target. As argued throughout this chapter, the relationship between cyber offending and technology is multifaceted, coproducing, and deeply intertwined. By applying a theoretical lens of Actor-Network Theory (Latour, 2007), the role and agency of the technology itself can be brought to the centre of the analytical frame. Through this lens, the role of technology as an active agent becomes visible. “Actor-Network Theory helps to explain how socio-technical ‘humanchine’ networks (comprised of humans and technologies as actors) intersect through translation and create agency” (Luppicini, 2014, 37). Data are the “scripts” that describe what objects – in this case, technology, software, and machines – ‘make’ “others – humans or non-humans – do” (Latour, 2007, 79). Surveillance and data

collection are the “artificial situations… devised to reveal [the] actions and performations” of objects (Latour, 2007, 79). The technological developments of the internet, cloud computing, e-commerce, cryptocurrency, mobile devices, etc. are active objects and agents which incentivise and necessitate people to act, interact, and communicate in certain ways. Our dependency on technology empowers it to control our behaviour in many ways. Applying an Actor-Network framework, these technologies are understood to be actors in a network and their interactions with people create meaning and agency (Luppicini, 2014, 37). Just as our law-abiding behaviour is shaped by the confines and possibilities of technology, so too is our illicit activity.

Actor-Network Theory further helps broaden the criminological lens by understanding the social dynamics of darknet forums, cybergangs, and ransomware groups. Many of these individuals or groups do not perceive themselves to be ‘criminal’ in the same way a murderer is. Many of the ransomware group pages list their victims as ‘partners’ or ‘clients’ whom they serve by revealing vulnerabilities in their systems. The nature of the anonymous online environment and cyber world online creates networks of offenders who are “psychologically, socially and physically further removed from their offences and victims, encounter fewer and/or less severe consequences for their behaviours and are likely to repeat these offences, emboldened by their experience” (Curtis and Oxburgh, 2022, 585). From an outside point of view, this perspective is difficult to reconcile with the havoc, damage, and pain that is brought upon the world and lives of many every day by cybercrime offending. Yet, Actor-Network Theory is helpful for understanding the social order that exists and enables offenders within networks; meaning and social order are created through human and technology agents alike,

and when this meaning is derived from coding language, the distanced relationship between crime and impact is visible (Luppicini, 2014).

With Actor-Network Theory, the traditional understanding of the cyber victim can be reconceptualized. Relying on Actor-Network theory, Wagen and Pieters argue for a novel framework for cyber victimization, referred to as hybrid victim theory (2020). They highlight "the blurry boundaries between humans and non-humans, tools and guardians, and offenders and victims" (Wagen and Pieters, 2020, 492). Wagen and Pieters' hybrid victim theory "views victimization not as a concrete event but as a complex interplay between (human and non-human) programmes of actions and anti-programmes" (2020, 492). Furthermore, hybrid victim theory outlines three main concept which allow for a reconceptualization of victims within (and by extending) Actor-Network theory (Wagen and Pieters, 2020). First, victim composition conceptualizations the victim as a human-technical hybrid network whereby victimhood and vulnerability are distributed as opposed to static (Wagen and Pieters, 2020). Second, victim delegation relates to the malleable and complex roles in the victimization process allowing victimhood analysis to encompass "the contributions of any (human or non-human) entity in the network" including technology and offenders (Wagen and Pieters, 2020, 491). Third, victim translation specifically focuses on the transformative, interactive, and dynamic condition of victimization (Wagen and Pieters, 2020). Thus, hybrid victim theory allows the conceptualization and analysis of the complex process of cybercrime through an understanding of victimhood which transcends risky or vulnerable behaviour and includes the interactive network of offenders, technology, and victims (Wagen and Pieters, 2020). Of course, this theory does not wholistically explain criminal or deviant behaviour; however, it does offer a valuable understanding of the trends toward cybercrime and explanations of how

and why individuals, who may otherwise not, commit traditional crimes hurting thousands or millions of people. Technology is the agent which allows an individual offender, who may never rob millions or invade the privacy of millions, do to so through the distancing conduit of a computer or malware. In this way, the technologies of the digital age can be understood as active agents, along with humans, in a network of meaning generation and social ordering which creates and reproduces the world of cybercrime offending.

Chapter 3: Law Enforcement, Security, and Cybercrime

The continuous rise in cybercrime offending, propelled by technological advancements, creates a need for cyber security and law enforcement. The cycle of technological growth and innovations enabling cyber offending extents to necessitate and facilitate policing practices to address, prevent, and deter crime. In this way, as with traditional forms of crime, policing is a retroactive and responsive mechanism to criminal activity. This exists on formal and informal levels. On a formal level law enforcement, police, and the law respond to new forms of crime. On an informal level, cyber security, social practices, and private organizations adapt to protect against and mitigate cyber threats. Yet, this also occurs in a proactive manner. Police, private organizations, and individuals actively pursue a more secure cyber world. Thus, the cybercrime environment is distinctive in the way that enforcement and security techniques and methods not only respond to cybercrime but also develop and advance with it as they rely on many of the same technological mechanisms. This does not mean that law enforcement efforts in the cyber realm are without challenges. Cybercrime poses many unprecedented difficulties for law enforcement. When technology is

brought to the centre of the analytical frame, however, a novel criminological relationship is visible where many of the same tools that facilitate offending also empower enforcement.

In this chapter, I argue that technology constructs a distinct and intricate criminological cyber landscape in regard to security and enforcement. First, I look at the current landscape of cyber policing and security by analysing how the technologies that enable cyber offending also enable cyber enforcement, security, and policing on a formal and informal level. Specifically, I focus on technologies of big data, cryptocurrency and blockchain, and mobile communication and networks. I also look at the ways police and private industries utilize cybercrime networks and social ordering to their advantage. Second, I discuss the novel challenges cybercrime and security pose to law enforcement and their approach to overcoming these challenges. Third, I centre technology in the analytical frame to understand the novel landscape of security, policing, and enforcement in the world of cybercrime.

Technological Enablers of Cyber Security, Policing, and Law Enforcement

The technological revolution comes along with the advent and massive growth of cybercrime, as demonstrated in Chapters 1 and 2. At the same time, it is also accompanied by a significant increase in cyber security, policing, law enforcement, and legal mechanisms for addressing cybercrime. This occurs in the formal sphere on the international, state, and local levels. In the informal sphere, it extends across the cyber security industry, corporations, social practices, and individual behaviours. On the stage of international justice, global attention turns toward the cyber world with milestone events such as the 2001 Budapest Convention on Cybercrime. Moreover, nations continue to focus on and put funding toward

addressing cybercrime both within and beyond their borders. For example, the Conflict, Stability and Security Fund (CSSF), a fund to address conflict and instability overseas created by the UK government, put more than 25.5 million pounds toward the "Global Cyber Programme, the African Join Operations Against Cyber Crime and bolstering the cyber defences [in] Georgia, Iraq, and elsewhere" in 2023 (Cabinet Office and UK Integrated Security Fund, 2024). On the private or informal side, not only do businesses, organizations, and individuals attend more to the risks of cybercrime, but the industry of cyber security drastically expands. Cyber security is now a leading industry around the world (Statista, 2023).

Across the board, the same technologies that are used to perpetrate cybercrime are also used to prevent, deter, and address it. Law enforcement agencies often use big data tools and analytics to guide proactive policing strategies (Tretyakov and Golyatina, 2022). Furthermore, artificial intelligence (AI) is utilized to combat cyber fraud; for example, a platform called Bitfury Crystal is used by the Netherlands to "analyse and detect suspicious cryptocurrency transactions" (Tretyakov and Golyatina, 2022, 13). In the United States, cryptocurrency analysis platforms document and track criminal transactions, and the FBI uses a system called Mayhem to identify hacking patterns, detect attacks, and locate offenders (Tretyakov and Golyatina, 2022). These systems reflect the ways in which law enforcement uses data analysis and AI to detect, prevent, and address cybercrime. Big data technologies are also used by corporations to detect and prevent fraud and other forms of cybercrime. For example, banking and payment systems such as Visa, MasterCard, and PayPal conduct anti-fraud analysis where they use data to create profiles for users "as a basis for assigning a potential fraud risk level" (Tretyakov and Golyatina, 2022, 13). Researchers and engineers continually pursue advances

in software to detect and prevent malware; for example, Andronio and colleagues study the detection performance of hardware detector technology which is used to detect malware on smartphones, and find a significant reduction in false positives and improvement in detection time (2015). In this way, the digitalization of the modern world and big data technologies not only foster and create avenues for cyber offending (see Chapter 2) but they also create avenues for cyber security, policing, and enforcement.

At the same time as blockchain enables cybercrime offending and illegal online transactions through cryptocurrency, it can also be a tool for tracking criminal transactions and activity. In a two-year study of ransomware payments, Huang and colleagues utilize a tracking of bitcoin to conduct end-to-end measurement of the ransomware ecosystem and infrastructure (2018). These researchers "follow the money trail from the moment a victim acquires bitcoins, to when ransomware operates cash them out" and make "a lower-bound estimate on ransom payments' volume of $16 million USD, made by 19,750 potential victims over two years" (Huang et al., 2018, 618). The decentralized technology of blockchain that chronicles the transactions in a digital ledger makes such tracking possible. This dual nature of cryptocurrency technology creating a unique offending-enforcement relationship in the world of cybercrime is further illustrated by the case of the Silk Road. Created in 2011 and shut down in 2013, the Silk Road reflects an international, online, darknet marketplace on the Tor network that uses bitcoin for the purchase and sale of illegal goods and services (Elgan, 2023). A study on the Silk Road marketplace, collecting data over eight months between 2011 and 2012, finds that the average total sales volume is over $1.2 million USD and "that Silk Road operates collect, an average, roughly 92,000 USD per month in commissions" (Christin, 2013, 220). An FBI investigation is responsible for shutting down the Silk Road and arresting

the site's administrator, Ross William Ulbricht (aka Dread Pirate Roberts), who is serving a life sentence without parole after his conviction in 2015 (Elgan, 2023; Maras, 2013). As with most darknet forums, the Silk Road transactions operate on Tor networks that conceal the IP addresses of its users. The anonymity of Tor networks presents a challenge for law enforcement efforts. However, the bitcoin transactions are recorded on public ledgers which allow them to be monitored and traced by authorities and police (Investopedia, 2023). This allows the authorities to seize bitcoin used in cybercrime, and in the Silk Road takedown, the FBI seize around 144,000 bitcoins which is valued at $34 million (at the time in 2013) (Ball et al. 2013; Investopedia, 2023). This seizure includes Ulbricht's 26,000 bitcoins (valued at $3.6 million at the time) (Ball et al. 2013; Investopedia, 2023). In this way, cryptocurrency and its technology are not only a catalyst for cybercrime but also for police and law enforcement to address cybercrime.

Online forums for communication, social media, mobile networks, and smartphones are also technological tools of the digital age which simultaneously propel offending and enforcement. The widespread use of the internet, mobile networks, and smartphones allows cybercrime to cascade across the world on a global scale. Yet, this interconnectedness of the digital world also allows for rapid law enforcement response as well as rapid alert systems to the public. While anonymous users access darknet forums for criminal activity, law enforcement can also monitor these Tor sites to track emerging malware, key criminal players, and activity. Likewise, internet activity, communication, and mobile networks can be targets for hacking, but they can also be resources for law enforcement as they gather intelligence, monitor online security, and collect evidence for criminal cases. Law enforcement is able to penetrate the criminal networks of the cyber world through anonymous online darknet

profiles. In this way, the policing of the digital age is able to utilize the online nature and the social ordering of digital criminal networks to their advantage.

Just as police and law enforcement gather confidential informants and use criminal networks to their advantage, the private cyber security industry does so as well. Businesses embrace 'bug bounty' programs where they offer monetary rewards to individuals who can identify flaws, vulnerabilities, issues, and bugs in their cyber systems (Gordon, 2023). For example, Epic Games, a video game developer, offers an average of $500 to hackers awarding "a total of $3.16 million to more than 550 people" as of October 2021 (Gordon, 2023). Bug bounty programs attract 'white hat' hackers and offer businesses an affordable avenue for cyber security through crowdsourcing (Gordon, 2023). Other major companies, such as Spotify, Slack, Starbucks, and Uber, use similar practices (Gordon, 2023). Law enforcement agencies develop similar programs. The United States Department of Defense is one such example which conducted a 'Hack the Pentagon' initiative in 2016 (DOD News, 2021). Following the success of that initiative, the Defense Digital Service offers a 'bug bounty' program, which is overseen by the Department of Defense Cyber Crime Center, and it "allows for research and reporting of vulnerabilities related to all [Department of Defense] publicly-accessible networks, frequency-based communication, Internet of Things, industrial control systems" (DOD News, 2021). 70% of the 29,000 vulnerability reports from this program are determined to be valid (DOD News, 2021). These bug bounty programs reflect how law enforcement and private cyber security utilize the networks of the cyber world to their advantage.

The Challenges of Cybercrime and Security for Law Enforcement

Just as the technologies of the digital age enable law enforcement to combat cybercrime, they also pose significant challenges. Technology and the digital age enable crime to be online, anonymous, invisible, and international. The advent of the internet and computers allows crime to occur at a scale and pace previously unimaginable. Offenders can commit crimes remotely from almost anywhere in the world. The digital world and its technologies change and evolve at a rapid rate. The result for law enforcement is immense challenges to prevent and address this crime, bring criminals to justice, and maintain the security and rights of the public. It is no easy task. The digitization of the majority of social and economic life is accompanied by the digitization of crime, and this necessitates the digitization of policing. The digital age is witness to the creation of agencies, task forces, and organizations that specialize in cyber. Examples of this include the United States' National Cyber Investigative Joint Task Force in 2008 and the United Kingdom's National Cyber Security Centre in 2016 (Boes and Leukfeldt, 2017). The international nature of cybercrime further necessitates global collaboration; as stated by the IMF, "the global nature of the dark web makes international cooperation imperative" (Kumar and Rosenbach, 2019). This necessity leads to the creation of international organizations and agencies such as the European Union's European Cybercrime Centre and the Joint Cybercrime Action Taskforce in 2013 (Boes and Leukfeldt, 2017). Across the globe, international law enforcement efforts take up the challenges posed by cybercrime.

The visibility (or lack thereof) of cybercrime poses a critical challenge to law enforcement and police. Visibility plays a role across multiple dimensions of cybercrime: 1) the visibility of the crime to victims, 2) the visibility of the crime to police and law

enforcement authorities, and 3) the visibility of police and law enforcement to current or potential offenders. With cybercrime, there lacks a physical manifestation of a crime that is often present with traditional offending. Unlike many forms of traditional crime, "cybercrime offenders hide their crimes through anonymous interactions with victims' devices or accounts, often through spoofed or anonymized networked connections" (Dodge and Burruss, 2019, 339). The digital and anonymous nature of cybercrime creates offending that is often subterranean and not blatantly visible to victims or the authorities. This is compounded by the "asynchronous nature of cybercrime" which enables an offence to occur "months before the victim is even aware of the cyberattack" (Dodge and Burruss, 2019, 339). You won't necessarily know your data is compromised or stolen until you see fraudulent charges, for example. It is the anonymous, asynchronous, and digital nature of cybercrime that allows it to be invisible and makes it difficult to investigate.

Furthermore, empirical research shows that "victims of cybercrime are less likely than those of traditional crime to report their victimisation to the police or other authorities" (Curtis and Oxburgh, 2022, 580). Victim non-reporting of cybercrime is due, in part, to perceptions that police are "unprepared for cybercrime" and "unlikely to act on a report" (Curtis and Oxburgh, 2022, 580). Underreporting of cybercrimes makes investigating and addressing cybercrimes difficult especially for lower levels of cybercrimes which only target one or a select few individuals. The third dimension of visibility affecting cyber enforcement is how visible police and authorities are to potential and current offenders. The thought of police conjures for most the image of a uniformed officer, the idea of street crime, patrol cars, etc. In many regions of the world, law enforcement demonstrates a physical, visible presence whether it be on the street, in cars, or at airports. The visible reminder of law is a central

component of many of the traditional forms of police activity to maintain order, provide security, and control crime. This component is largely lost on the cyber streets. How do you establish a police presence online? How do you patrol the darknet? The potential deterrent effect of cyber policing is discussed further in the next section.

Even when the crime is known and the enforcement entities or individuals are technologically equipped to do their job, the international nature of cybercrime is a critical barrier for law enforcement and police. Not only are the logistics and practicalities geographical widespread crime challenging, but all of the difficulties that accompany foreign relations and international politics also come along with international cybercrime making it hard to investigate and prosecute. Many law enforcement agencies are constrained to the jurisdictions of national boundaries (Doyle, 2023). Of course, this makes cross-border cybercrime more appealing to threat actors. As noted by Doyle, "cybercrime is almost always a cross-border event, with criminals targeting victims in foreign countries to reduce the risk of arrest" (2023). While this limits law enforcement efforts to address cybercrime, there are prominent examples of internationally cooperative efforts to combat cross-border cybercrime attacks. In 2017, two international law enforcement operations orchestrate the coordinated takedown of prominent darknet sites AlphaBay, (Operation Bayonet) led by the FBI, and Hansa Market, (Operation GraveSac) led by the Netherlands National High Tech Crime Unit (NHTCU) (Afilipoaie and Shortis, 2018). Europol plays a central role in coordinating these efforts with law enforcement authorities in the United States, Netherlands, the United Kingdom, Thailand, Canada, Lithuania, and France (FBI, 2017). Europol reports that 12 different agencies collectively plan and agree to the operations, and during the critical time of

the joint operations, Europol hosts a command post to coordinate with representatives from different agencies (Europol, 2017).

Although these began as separate operations, their success is reflected in how they coordinated. By applying a strategy previously used by the FBI to take down a child abuse darknet site in 2015 called Playpen, NHTCU "seize direct control of the Hansa cryptomarket" in order to run the site as administrators and be the most effective in stopping its operation while also catching major players (Jardine, 2021). They accomplish this by locating its servers; usually an extremely difficult endeavour because of the anonymous nature of the darknet and Tor networks, the NHTCU track a bitcoin wallet address revealed in an online chat between two key suspects (Jardine, 2021). Tracing the blockchain to the payment provider and leveraging them to uncover the physical location (Lithuania) of the servers for Hansa, the NHTCU set up a link to copy the Hansa database in their jurisdiction and takes over administration of the site in June 2017 (Afilipoaie and Shortis, 2018; Jardine, 2021). The takedown of AlphaBay occurs on July 5th and the site administrator, a 25-year-old named Alexandre Cazes going by the username, alpha02, is arrested in Thailand to be extradited to the US (Afilipoaie and Shortis, 2018). No public announcement of Operation Bayonet's success is announced at the time and speculation among users assumes an exit scam by the site's administrators (Afilipoaie and Shortis, 2018). This results in the influx of users to Hansa, and the NHTCU, secretly acting as the site administrators decides to do a temporary pause on registration to deal with the influx and continue operations; this type of temporary close on registration in the face of waves of new users when rival markets close is a common cryptomarket practice (Afilipoaie and Shortis, 2018).

On July 20th 2017, the Dutch authorities shut down Hansa (Europol, 2017). During the 27-day covert operation of Hansa, the NHTCU monitor about 1,000 daily transactions and gather a total of about 10,000 foreign addresses of market buyers (Afilipoaie and Shortis, 2018; Europol, 2017). The Dutch authorities are able to pass this information on to Europol to coordinate further enforcement efforts (Europol, 2017). The FBI reports that around the time of its takedown, AlphaBay had more than 250,000 illegal drug listings, with 122 vendors advertising Fentanyl and 238 vendors advertising heroin, and more than 100,000 listings for fraudulent identification documents, malware and hacking tools, firearms, and counterfeit goods (FBI, 2017). Furthermore, the FBI reports that between 2015 and 2017, "more than $1 billion in illegal transactions in bitcoin and other cryptocurrencies" occurred on AlphaBay (FBI, 2017). On the whole, these joint operations dismantle a substantial corner of the darknet marketplace at the time (Europol, 2017; FBI, 2017). Although the closing of one criminal marketplace is usually accompanied by the rise of others, major shutdowns like these can disrupt cybercrime offending by increasing fear of law enforcement and by decreasing perceived convenience through reduced trust and reliability (Bradley, 2019). The long-term success and the potential deterrent effect of such law enforcement efforts are discussed further below.

These operations reflect successful international coordination, technologically enabled policing, and innovative law enforcement strategies. These include examples of utilizing the same technologies that enable cybercrime, infiltrating cyber networks and darknet forums, international coordination, and making law enforcement efforts visible to offenders. To gain control of Hansa, the NHTCU utilizes blockchain technology, which is critical in cryptocurrencies such as bitcoin, to uncover the physical location of the servers hosting the

site (Afilipoaie and Shortis, 2018). The successful and covert administration of Hansa by the NHTCU is a landmark success of covert cyber policing; acting as the site administrators for 27 days without raising substantial or widespread suspicion is an impressive endeavour in undercover cyber policing and allowed for the collection of critical information and evidence (Afilipoaie and Shortis, 2018). These operations involve major international cooperation across several countries which allowed for the strategic coordination of the successfully successive shutdown of both sites while gathering maximum information on threat actors through a 'honeypot' tactic (covert operating of the site) with Hansa following the FBI takedown of AlphaBay (Afilipoaie and Shortis, 2018). The information gathered through this strategy allows for positive cascading effects such that critical details on threat actors are disseminated to other law enforcement agencies and Europol allowing for secondary joint action (Afilipoaie and Shortis, 2018; Europol, 2017). Examples of this are evident in law enforcement efforts in the months following the takedown including the "knock-and-talks" conducted by the United States and Netherlands whereby Hansa users were visited by authorities, "informed that their addresses had been compromised in the Hansa bust, and warned to stay away from cryptomarkets" (Afilipoaie and Shortis, 2018, 4). Moreover, notices of the seizure are posted on the darknet sites following the operations (FBI, 2017). These posts and 'knock-and-talk' actions allow law enforcement agencies to have a more visible presence in the cyber world. It is a form of cyber enforcement in the digital age that allows officers and agents of law to police the cyber streets.

Operation Bayonet and Operation GraveSac represent novel policing tactics and strategies and major international law enforcement coordination and cooperation (Europol, 2017). Throughout the joint effort, law enforcement and police utilize technologically enabled

cyber policing in regard to their coordinated approach, technically sophisticated tools, and highly effective strategy which reflects a high degree of competence in and understanding of cybercrime operations, cyber networks, online communities, and individual threat actors. This case study reveals how the technologies of the digital age (e.g., blockchain, anonymous Tor networks, darknet forums and marketplaces, etc.) not only enable offending (see Chapter 2) but also enable enforcement. This case further demonstrates how the unique dynamics, social ordering, and networks of the cyber world pose unprecedented challenges to police and law enforcement. At a high level, on a national and international scale, law enforcement is readily able to take on these challenges and implement adaptive, innovative, and technologically sophisticated policing tactics. Operation Bayonet and Operation GraveSac demonstrate the cyber policing that is mandated and necessitated by the problem of cybercrime. Yet, this race against the growing threat of cybercrime is ongoing.

Frameworks of Cyber Policing in the Digital Age

Using Actor-Network Theory (Latour, 2007) to centre technology in the analytical frame, the multifaceted cycle of progress described in Chapter 2 can be extended to include formal (government / law enforcement) and informal (corporate / individual) cyber security. With an Actor-Network approach, those in the fields of cyber policing, law enforcement, and security can be included along with cyber offenders, victims, and the technologies of the digital age as actors of an interconnected network of change, information, and meaning generation that creates the reality of the cyber world. As technologies of the digital age (e.g., those of cryptocurrency, big data, and mobile communication) propel cybercrime as tools, targets, and models of offending, they also propel cyber security and policing as resources,

evidence, and methods for prevention, detection, investigation, and enforcement. This cycle is further complicated by the demand for security and policing that is mandated by the increase in cybercrime. Finally, the cycle reproduces itself as cyber criminals, law enforcement agencies/organizations/taskforces, and the cyber security industry develop innovative technological advancements to further their efforts. The dynamic of crime is changed on a fundamental level when criminal innovation becomes synonymous with police innovation and vice versa. This analytical frame is particularly helpful when looking at cyber law enforcement and security because it reveals how technological competence and expertise play an active role in the success of law enforcement and cyber security efforts.

This success is evident on a large-scale, transnational effort where the law enforcement efforts are readily able to tackle the challenges posed by cybercrime. International cooperation, coordination with private cyber security companies, technological sophistication, and cybercrime expertise require immense specialization and resources. When these resources are available, law enforcement efforts are successful, as with Operation Bayonet and Operation GraveSac. The long-term impacts of these large-scale, transnational operations, even when successful, is debated by scholars. For example, many scholars argue that the takedown of darknet forums and marketplaces does not significantly disrupt the cybercrime ecosystem in the long term because new markets emerge and users migrate to those forums (Chawki, 2022). Yet, other scholars find that law enforcement efforts are effective in deterring cybercrime offenders and darknet marketplace users not only within the countries of those offenders arrested but also beyond those national jurisdictions (Chan et al., 2023). Other research indicates that large-scale operations and takedowns increase fear of law enforcement and decrease darknet user activity by degrading perceptions of the legitimacy

and reliability of darknet forums and marketplaces (Bradley, 2019). In this way, creating cyber policing visibility may provide a deterrent effect in addition to the immediate benefits of taking down major illegal online marketplaces; however, the resilience of the cybercrime ecosystem overall in the face of major, successful law enforcement efforts remains contested.

However, disseminating these practices to the local level to address relatively smaller forms of cyber offending is yet to be seen. While national and international agencies present a strong and innovative defence and shield against major cybercrime (e.g., large-scale ransomware and DDoS attacks, state-sponsored hacking, major darknet forums and marketplaces, and high-threat hacker groups), technological sophistication of cybercrime presents a challenge for enforcement on a local level. In the United States, for example, "state and local governments [are] largely hesitant to tackle [cybercrime] enforcement" (Brunner, 2019, 563). While the scale and impact of relatively smaller cybercrimes may also be smaller, the challenges for law enforcement remain large. The technical, anonymous, asynchronous, and international nature of cybercrime remains for even relatively lower levels. As a result, many relatively low-level cybercrimes remain unaddressed, many individual victims remain invisible, and therefore a substantial amount of cybercrime remains in the dark figure of crime. The traditional model of local policing on the street to "keep the 'dangerous classes' off the streets through a dual mandate to keep the peace and bring felons to justice" is challenging to apply to cyber space (Wall, 1998, 211). In a 2013 qualitative study of cybercrime investigations at the state and local level in the United States, Lemieux and Bales find that cybercrime is largely investigated in a traditional "complaint-led model of policing rather than an intelligence-led" and prioritized based on national directives and administrative necessities (2012, 76). This model is described by participants despite their characterization of

the cybercrime threat, as significant in regard to "its scope (national and international) and magnitude (volume and consequences)" which would otherwise mandate the latter model as with organized crime and terrorism (Lemieux and Bales, 2012, 76). As this research and preceding sections of this chapter reveal, cyber policing is proactive and intelligence-led at a high, transnational level but reactive and complaint-led at the local level.

Effective policing of cybercrime at the local level is constrained by limited resources and cyber specialization (De Paoli et al., 2020; Kewkes and Andrews, 2006). While traditional models of more local law enforcement require officers to be generalists who police the streets to maintain order, address crime, and provide security, cybercrime necessitates specialists with expertise in technology and sophisticated computer science knowledge (Harkin et al., 2018). Even those countries with extensive cyber law enforcement setups struggle with a scarcity of qualified personnel and experienced expertise necessary for addressing cybercrime because salaries in the private sector are almost always higher than those in the public sector (Chawki, 2022). Translating the high-level, international law enforcement practices that are effective and successful at addressing larger cybercriminal operations to a more local level is particularly challenging because the challenges posed by smaller-scale cybercrime exist across the scale of crime, but resources to address them do not. Cybercrime perpetrated by a single offender and impacting a single victim may still be committed across borders and use sophisticated technology. However, the resources to gather evidence, track or identify the perpetrator, and initiate the international cooperation required to apprehend and prosecute the offender are lacking.

Conclusion

The contemporary landscape of society is revolutionized by technology. A process of digitization sweeps across the world. Data is now the fundamental and universal language of many of our social and economic interactions. Using a Marxist approach to make data analogous with capital, datafication can be seen to manifest an infinite process of data capital accumulation, dispossession, and appropriation (Couldry and Mejias, 2019; Sadowski, 2019; Thatcher et al., 2016). In the process of data capital accumulation, our daily lives are monitored and monetized. This process drives technological development. However, there is a dark side to technology; its productive and positive use is matched by its malicious and criminal use. Technologies of big data, cryptocurrency and the digital economy, and online and mobile networks enable crime as tools and targets for offending. Cyber offending then necessitates cyber security, policing, and law enforcement efforts to address that crime. The cycle repeats as cybercrime and cyber security drive further technological innovation.

Two critical technological paradoxes are brought to light. First, inherent in the process by which technologies propel us into the future is the malicious and criminal (mis)use of those technologies. Second, those technologies are a catalyst for both cybercrime and cyber security and policing. This creates an unprecedented dynamic for law enforcement and police. Just as cybercrime fundamentally differs from more traditional forms of crime, the cyber policing that it mandates fundamentally differs from traditional forms of policing. Technology creates a novel relationship between offenders and enforcement; their interactions (or lack thereof) differ, their conceptions of risk (on both sides) shift, and the environments for engagement alter. The scale, scope, and context of crime and policing drastically change in the cyber world. Technology is reshaping the tools, methods, and targets of both cyber offending and

cyber policing in the digital age. Law enforcement is facing the exceptional challenge of scaling the successful proactive approach of addressing large-scale international cybercrime down to the local level to combat the smaller-scale cases of cyber offending. A cultural shift toward cyber literacy and cyber specialization, for both individuals seeking digital security and law enforcement aiming to address crime, is mandated by cyber offending.

The analysis and investigation throughout the preceding pages beg the question: is the digital age a replication of reality onto a cyber environment? Are the innately human paradigms of development, crime, and enforcement simply playing out online? Are the economic, social, and regulatory functions simply transitioning to cyber space? While many of our actions and interactions, can exist in the online environment, they are fundamentally changed in this setting. When technology mediates our society, economy, and communication, it also impacts them. Just as technology can be centred to derive insights into the world of cybercrime, so too can cybercrime to derive insights into technology. Through the lens of cybercrime, the boundless progression of technological dependence, influence, and datafication is visible. Extending the Actor-Network framework (Latour, 2007) to analyse cybercrime offending and enforcement, the pervasive and active role of technology is evident. It is far from the neutral, impartial, and benign facilitator of human activity it often appears to be. What is made clear is that technology is not an armature of the idealistic human civilization of the future. Instead, it is a deeply biased, partial, and positioned actor that acts on, through, or with other objects and beings. Today, you don't have to look far to see examples of this; internet searchers bring up AI (LLM) responses with often outrageous or false information. As much as we make technology, it makes us. The self-perpetuating cycle discussed in this paper illustrates the potential benefits and the dangers of the role of

technology. Technology reveals the unique landscape of cybercrime as much as cybercrime reveals the true nature of technology. Inherent in its use is its misuse.

Bibliography

Abbate, J. (1999) *Inventing the internet*. Cambridge, MA: MIT Press.

Afilipoaie, A. and Shortis, P. (2018) "Crypto-market enforcement-new strategy and tactics", *Policy*, *54*, pp. 87-98. https://cointhinktank.com/upload/Crypto-Market-Enforcemnet-New-Strategy-and-Tactics.pdf.

Aiyer, B. *et al.* (2022) *New survey reveals $2 trillion market opportunity for cybersecurity technology and Service Providers*, *McKinsey & Company*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers.

Andronio, N., Zanero, S., and Maggi, F. (2015) "Heldroid: Dissecting and detecting mobile ransomware", in *Research in Attacks, Intrusions, and Defenses: 18th International Symposium, RAID 2015, Kyoto, Japan, November 2-4. Proceedings 18*, pp. 382-404. Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-319-26362-5_18.

Austin, J.R., (1999) "The Law of Electronic Commerce and Digital Signatures: An Annotated Bibliography", *UIC John Marshall Journal of Information Technology & Privacy Law*, *17*(3) 12.

Ball, J., Arthur, C., and Gabbatt, A. (2013) *FBI claims largest bitcoin seizure after arrest of alleged Silk Road founder*, *The Guardian*. https://www.theguardian.com/technology/2013/oct/02/alleged-silk-road-website-founder-arrested-bitcoin.

BBC News (2021) *The lazarus heist: How North Korea almost pulled off a billion-dollar hack*, *BBC*. https://www.bbc.co.uk/news/stories-57520169.

Bearman, J. (2020a) *The untold story of silk road, part 1*, *Wired*. https://www.wired.com/2015/04/silk-road-1/.

Bearman, J. (2020b) *The untold story of silk road, part 2: The fall*, *Wired*. https://www.wired.com/2015/05/silk-road-2/.

Billion Dollar Heist (2023) Directed by Daniel Gordon and Brendan Donovan [Film].

Boes, S., Leukfeldt, E.R. (2017) "Fighting Cybercrime: A Joint Effort", in Clark, R., Hakim, S. (eds) *Cyber-Physical Security: Protecting Critical Infrastructure, at the State and Local Level*. vol 3. Springer, Cham. https://doi.org/10.1007/978-3-319-32824-9_9.

Borgeaud, A. (2023) *Cybersecurity spending worldwide 2022*, *Statista*. https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/#:~:text=Global%20cybersecurity%20spending%202017%2D2022&text=In%202022%2C%20total%20spending%20on,in%20the%20period%20under%20review.

Bradley, C. (2019) "On the resilience of the Dark Net Market ecosystem to law enforcement intervention", PhD diss., UCL (University College London). https://discovery.ucl.ac.uk/id/eprint/10080409/8/Bradley_10080409_thesis.pdf.

British Library (2024) *Learning Lessons from the Cyber-Attack: British Library Cyber Incident Review. British Library.* https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf.

Brunner, M. (2019) "Challenges and Opportunities in State and Local Cybercrime Enforcement", *Journal of National Security Law & Policy*. 10 (3), pp. 563-582. https://www.proquest.com/docview/2557267954?parentSessionId=3zwAthJdmMhatu

2VeaMpedwWJphkldG3qxskk%2F%2FDPuo%3D&pq-origsite=primo&accountid=13042&sourcetype=Scholarly%20Journals.
Cabinet Office and UK Integrated Security Fund (2024) *Huge boost for global security with almost £1 billion government investment*, *GOV.UK*. https://www.gov.uk/government/news/huge-boost-for-global-security-with-almost-1-billion-government-investment#:~:text=Last%20year%20it%20more%20than,defences%20Georgia%2C%20Iraq%20and%20elsewhere.
Cellan-Jones, R. (2015) *TalkTalk cyber-attack: Boss 'receives ransom email'*, *BBC News*. https://www.bbc.co.uk/news/uk-34615226.
Chan, J., He, S., Qiao, D., and Whinston, A. (2023) "Shedding light on the dark: The impact of legal enforcement on darknet transactions", *Information Systems Research*, *35*(1), pp.145-164. https://doi.org/10.1287/isre.2023.1222.
Chappell, B., and Neuman, S. (2017) *U.S. says North Korea 'directly responsible' for WannaCry ransomware attack*, *NPR*. https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack.
Chawki, M. (2022) "The Dark Web and the future of illicit drug markets", *Journal of Transportation Security*, 15(3), pp. 173-191. https://link.springer.com/article/10.1007/s12198-022-00252-y.
Christin, N. (2013) "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace", in *Proceedings of the 22nd international conference on World Wide Web*. pp. 213-224. https://dl.acm.org/doi/pdf/10.1145/2488388.2488408.
Cohen, L.E., and Felson, M. (1979) "Social Change and Crime Rate Trends: A Routine Activity Approach", *American Sociological Review* 44(4), pp. 588-608. https://doi.org/10.2307/2094589.
Comaroff, J., & Comaroff, J.L. (2012). "Theory from the South" in *Theory from the South: Or, How Euro-America is Evolving Toward Africa* (1st ed.). Routledge. https://doi-org.ezproxy-prd.bodleian.ox.ac.uk/10.4324/9781315631639
Coppola, D. (2024) *Amazon: Third-party seller share 2024*, *Statista*. https://www.statista.com/statistics/259782/third-party-seller-share-of-amazon-platform/.
Couldry, N., & Mejias, U. A. (2019) "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject", *Television & New Media*, 20(4), 336-349. https://doi.org/10.1177/1527476418796632.
Council of Europe (2001) *ETS No. 185-The Budapest Convention on Cybercrime*. https://rm.coe.int/1680081561.
Curtis, J., & Oxburgh, G. (2022) "Understanding cybercrime in 'real world' policing and law enforcement", *The Police Journal*, *96*(4), pp. 573-592. https://doi.org/10.1177/0032258X221107584.
De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M. and 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), pp.1429-1445. https://doi.org/10.1093/police/paaa027.

Deb, S. (2024) *Ticketmaster confirms data breach. here's what to know.*, *The New York Times*. https://www.nytimes.com/2024/05/31/business/ticketmaster-hack-data-breach.html.
Demirgüç-Kunt, A., Klapper, L., Singer, D., and Ansar, S. (2022) *The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19.* Washington, DC: World Bank. https://www.worldbank.org/en/publication/globalfindex.
DOD News (2021) *DOD expands hacker program to all publicly accessible Defense Information Systems*, *U.S. Department of Defense*. https://www.defense.gov/News/News-Stories/Article/Article/2595294/dod-expands-hacker-program-to-all-publicly-accessible-defense-information-syste/.
Dodge, C. and Burruss, G. (2019) "Policing Cybercrime: Responding to the Growing Problem and Considering Future Solutions", in Leukfeldt, R, & Holt, TJ (eds) *The Human Factor of Cybercrime*, Taylor & Francis Group, Oxford. https://ebookcentral.proquest.com/lib/oxford/reader.action?docID=5940226&ppg=356.
Doyle, S. (2023) *Cybercrime and violent crime are converging - this is why*, *World Economic Forum*. https://www.weforum.org/agenda/2023/10/cybercrime-violent-crime/#:~:text=Cybercrime%20is%20almost%20always%20a,they%20are%20by%20national%20boundaries.
Easterly, J. and Fanning, T. (2023) *The attack on Colonial Pipeline: What we've learned & what we've done over the past two years: CISA*, *Cybersecurity and Infrastructure Security Agency CISA*. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.
Elgan, M. (2023) *How the silk road affair changed law enforcement*, *Security Intelligence*. https://securityintelligence.com/articles/silk-road-dark-web-law-enforcement/#.
Europol (2017) *Massive blow to criminal dark web activities after globally coordinated operation*, *Europol*. https://www.europol.europa.eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.
FBI (2017) *Alphabay takedown*, *FBI*. https://www.fbi.gov/news/stories/alphabay-takedown.
Fleck, A. and Richter, F. (2024) *Cybercrime Expected to Skyrocket in Coming Years*, *Statista Daily Data*. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/.
Foley, S., Karlsen, J.R., Putniņš, T.J. (2019) "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?", *The Review of Financial Studies*, 32(5) pp. 1798-1853, https://doi.org/10.1093/rfs/hhz015.
Fortune Business Insights (2024) *Data Storage Market Size, Share & Growth Statistic*. https://www.fortunebusinessinsights.com/data-storage-market-102991#.
Freeze, D. (2023) *Cybercrime to cost the world $9.5 trillion USD annually in 2024*, *Cybercrime Magazine*. Ed by S. Morgan. https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/#:~:text=A%20breakdown%20of%20global%20cybercrime,%24182.5%20billion%20USD%20a%20week.
Gecsoyler, S. (2024) *Ticketmaster hit by Data Hack that may affect 560m customers*, *The Guardian*. https://www.theguardian.com/technology/article/2024/jun/01/live-nation-investigating-data-breach-of-its-us-ticketmaster-unit.

Gordon, B. (2023) *Why companies pay hackers big bucks to break their networks*, *GovTech*. https://www.govtech.com/security/why-companies-pay-hackers-big-bucks-to-break-their-networks#:~:text=Like%20Epic%2C%20Raleigh's%20fast%2Dgrowing,hackers%20who%20often%20work%20anonymously.

Greenberg, A. (2018) *The untold story of notpetya, the most devastating cyberattack in history*, *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Greenberg, A. (2024) *Ransomware payments hit a record $1.1 billion in 2023*, *Wired*. https://www.wired.com/story/ransomware-payments-2023-breaks-record/.

Greenwald, G., MacAskill, E., and Poitras, L. (2013) *Edward Snowden: The whistleblower behind the NSA surveillance revelations*, *The Guardian*. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Harkin, D., Whelan, C. and Chang, L. (2018) "The challenges facing specialist police cyber-crime units: an empirical analysis", *Police Practice and Research*, 19(6), pp. 519–536. https://doi.org/10.1080/15614263.2018.1507889.

Hicks, C. and Adams, M. (2024) *Different types of cryptocurrencies*, *Forbes*. https://www.forbes.com/uk/advisor/investing/cryptocurrency/different-types-of-cryptocurrencies/.

Highland, H. J. (1997) "A history of computer viruses — The famous 'trio'", *Computers & security*. 16 (5) 416–429.

Huang, D.Y., Aliapoulios, M.M., Li, V.G., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., Levchenko, K., Snoeren, A.C. and McCoy, D. (2018) "Tracking ransomware end-to-end", in *2018 IEEE Symposium on Security and Privacy (SP)*. pp. 618-631. IEEE. https://ieeexplore.ieee.org/abstract/document/8418627.

Investopedia (2023) *What was the Silk Road Online? history and closure by FBI*, *Investopedia*. https://www.investopedia.com/terms/s/silk-road.asp#:~:text=All%20trades%20on%20Silk%20Road,by%20legal%20and%20regulatory%20bodies.

Jardine, E. (2021) "Policing the cybercrime script of darknet drug markets: Methods of effective law enforcement intervention", *American Journal of Criminal Justice*, *46*, pp. 980-1005. https://link.springer.com/article/10.1007/s12103-021-09656-3.

Kaspersky (2024) "What is WannaCry ransomware?", *Kaspersky*. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry.

Koops, B.J. and Leenes, R., (2006) "Code and the slow erosion of privacy", *Mich. Telecomm. & Tech. L. Rev.*, *12*, pp. 115. https://doi.org/10.1080/1043946042000338922.

Kumar, A., and Rosenbach, E. (2019) *The truth about the dark web – IMF F&D*, *IMF*. https://www.imf.org/en/Publications/fandd/issues/2019/09/the-truth-about-the-dark-web-kumar.

Latour, B., (2007) *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press: New York.

Leiner, B. et al. (1997) *The past and future history of the Internet*. Vol. 40. New York: ACM. https://dl-acm-org.ezproxy-prd.bodleian.ox.ac.uk/doi/abs/10.1145/253671.253741.

Lemieux, F. and Bales, B. (2012) "Investigating transnational cybercrime: current challenges and emerging initiatives", in Leman-Langlois, S (ed.), Technocrime: Policing and Surveillance, Taylor & Francis Group, Oxford.

Leukfeldt, E.R., Kleemans, E.R. and Stol, W.P., (2017) "Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks", *The British Journal of Criminology*, *57*(3), pp.704-722. https://www-jstor-org.ezproxy-prd.bodleian.ox.ac.uk/stable/26780264?sid=primo.

Loebenberger, D. and Wielputz, R., (2006) "Evolution! from creeper to storm", in *Presentation for the Seminar on" Malware.* pp. 1-7. https://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/07ws/malware/evolution_report.pdf.

Luppicini, R. (2014) "Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research", *Global Media Journal: Canadian Edition*, *7*(1). https://epe.lac-bac.gc.ca/100/201/300/global_media_journal/v07n01/www.gmj.uottawa.ca/1401/v7i1_luppicini.pdf.

Lyngaas, S. (2023) *Exclusive: US Government agencies hit in Global Cyberattack | CNN politics*, *CNN*. https://edition.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html.

M. G. Porcedda and D. S. Wall, "Cascade and Chain Effects in Big Data Cybercrime: Lessons from the TalkTalk hack", *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Stockholm, Sweden, 2019, pp. 443-452, doi: 10.1109/EuroSPW.2019.00056.

Maras, M.H. (2013) *Inside darknet: The takedown of silk road*, *Centre for Crime and Justice Studies*. https://www.crimeandjustice.org.uk/publications/cjm/article/inside-darknet-takedown-silk-road.

Meteor Space (2023) Global Top Selling Online Marketplace statistics- Meteor Space, Meteor Space - Warehousing & Order Fulfillment Services in Ireland & Europe: Meteor Space. https://www.meteorspace.com/global-top-selling-online-marketplaces-all-the-statistics-you-need-to-know/.

Minnaar, A. & Reddy, E. (2018) "Cryptocurrencys: a tool and target for cybercrime", *Acta criminologica (Criminological Society of Southern Africa)*. 31 (3), pp. 71-92. https://journals-co-za.ezproxy-prd.bodleian.ox.ac.uk/doi/epdf/10.10520/EJC-14d902942d.

Moules, J. (2024) "Job number one is to think straight': how to manage a major cyber attack: The CEO. Roly Keating, British Library The former BBC executive brought the nation's book collection online — then disaster struck, writes Jonathan Moules", *The Financial times (London ed.)*. https://www.proquest.com/docview/2928710196?pq-origsite=primo&accountid=13042&sourcetype=Newspapers.

Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system. https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf.

Petrosyan, A. (2024a) *Internet and social media users in the world 2024*, *Statista*. https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=As%20of%20April%202024%2C%20there,population%2C%20were%20social%20media%20users.

Petrosyan, A. (2024b) *Number of data breaches and victims U.S. 2023*, *Statista*. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.
Reynald, D.M. (2019) "Guardianship in the digital age", *Criminal Justice Review*, *44*(1), pp.11-24. https://journals.sagepub.com/doi/full/10.1177/0734016818813693.
Richardson, R. and North, M.M., (2017) "Ransomware: Evolution, mitigation and prevention", *International Management Review*, *13*(1), pp.10-21. https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs.
Richter, F. (2023) "Charted: There are more mobile phones than people in the world", *World Economic Forum*. https://www.weforum.org/agenda/2023/04/charted-there-are-more-phones-than-people-in-the-world/.
Rydning, D.R.J.G.J., Reinsel, J. and Gantz, J., (2018) "The digitization of the world from edge to core", *Framingham: International Data Corporation*, *16*, pp.1-28. https://www.seagate.com/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.
Sadowski, J. (2019) "When data is capital: Datafication, accumulation, and extraction", *Big Data & Society*, 6(1). https://doi.org/10.1177/2053951718820549.
Safavi, S., Shukur, Z. and Razali, R., (2013) "Reviews on cybercrime affecting portable devices", *Procedia Technology*, *11*, pp. 650-657. https://www.sciencedirect.com/science/article/pii/S2212017313003952.
Saha, D. (2021) *Google cloud brandvoice: How the world became data-driven, and what's next*, *Forbes*. https://www.forbes.com/sites/googlecloud/2020/05/20/how-the-world-became-data-driven-and-whats-next/?sh=6ed3f2e457fc.
Schwartz, E. I. (1997) *Webonomics: nine essential principals [sic] for growing your business on the World Wide Web*. London: Penguin Books.
Searchlight Cyber (2024) *2023 in review: Hacking forums and Dark Web marketplaces*, *Searchlight Cyber*. https://www.slcyber.io/2023-in-review-hacking-forums-and-dark-web-marketplaces/.
Shanahan, M. and Bahia, K. (2023) *The State of Mobile Internet Connectivity 2023*. GSMA. https://www.gsma.com/r/wp-content/uploads/2023/10/The-State-of-Mobile-Internet-Connectivity-Report-2023.pdf?utm_source=website&utm_medium=button&utm_campaign=somic23.
Sherwood, H. (2024) *British Library begins restoring digital services after cyber-attack.* The Guardian. https://global-factiva-com.ezproxy-prd.bodleian.ox.ac.uk/ha/default.aspx#./!?&_suid=171708552822005107083381185404.
Spafford, E. H. (1989) *The internet worm program: an analysis*. Vol. 19. https://dl-acm-org.ezproxy-prd.bodleian.ox.ac.uk/doi/abs/10.1145/66093.66095.
Statista (2023) *Cybersecurity - worldwide: Statista market forecast*, *Statista*. https://www.statista.com/outlook/tmo/cybersecurity/worldwide#analyst-opinion.
Ström, T.E. (2022) "Data mining on the crawl frontier: Metaphor in cybernetic capitalism.", *Law Text Culture*, *26*, pp.123.
Sukhai, N. (2004) "Hacking and cybercrime", in *2004 Information Security Curriculum Development Conference, InfoSecCD 2004*. 2004 ACM. pp. 128-132. https://dl-acm-org.ezproxy-prd.bodleian.ox.ac.uk/doi/pdf/10.1145/1059524.1059553.

Tambe, N. and Jain, A. (2024) *Advantages and disadvantages of cryptocurrency in 2024*, *Forbes*. https://www.forbes.com/advisor/in/investing/cryptocurrency/advantages-of-cryptocurrency/.

Temple-Raston, D. (2021) *A 'worst nightmare' cyberattack: The untold story of the solarwinds hack*, *NPR*. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

Thatcher, J., O'Sullivan, D., and Mahmoudi, D. (2016). "Data colonialism through accumulation by dispossession: New metaphors for daily data", *Environment and Planning D: Society and Space*, 34(6), 990-1006. https://doi.org/10.1177/0263775816633195.

The White House, Office of Management and Budget (2024) "15. Information Technology and Cybersecurity Funding", in *Analytical Perspectives: Budget of the U.S. Government, FY 2025*. U.S. Government Publishing Office: Washington. https://www.whitehouse.gov/wp-content/uploads/2024/03/ap_15_it_fy2025.pdf.

Tretyakov, V., and Golyatina, S. (2022). "Applying Big Data technologies to counter cyber fraud", *Amazonia Investiga*, *11*(49), 9-16. https://doi.org/10.34069/AI/2022.49.01.1.

United Nations, Office on Drugs and Crime (2004) *United Nations Convention Against Transnational Organized Crime*. United Nations: New York. https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.

Vashisht, S., Gupta, S., Singh, D. and Mudgal, A., (2016) "February. Emerging threats in mobile communication system", in *2016 International conference on innovation and challenges in cyber security (ICICCS-INBUSH)* (pp. 41-44). IEEE. https://ieeexplore.ieee.org/abstract/document/7542341?casa_token=rhUGX-Ea1CMAAAAA:HhNAgBjpuwSyk6W3RdT1FJEv1xHLiDptKbwUyM9Bavy9wwszeBVzs4IdBxpBPJj1ujNQcBgQ.

Wagen, W.V.D., and Pieters, W. (2020) "The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory", *European Journal of Criminology*, 17(4), pp. 480-497. https://doi.org/10.1177/1477370818812016.

Wakefield, J. (2017) *Tax software blamed for cyber-attack spread*, *BBC News*. https://www.bbc.co.uk/news/technology-40428967.

Wall, D. S. (1998). Catching Cybercriminals: Policing the Internet. *International Review of Law, Computers & Technology*, *12*(2), pp. 201–218. https://doi.org/10.1080/13600869855397.

Wall, D.S. (2018) "How Big Data Feeds Big Crime." *Current History* 117(795) pp. 29-34. https://www.jstor.org/stable/48614313.

Appendix

TABLE 1: ACRONYMS AND TECHNICAL TERMINOLOGY

TERM	Meaning	Citation
AI	AI stands for Artificial Intelligence. It is a term used to refer to a broad category of systems, software, or machines that perform "intelligent", automated services or functions. The AI tools that currently captivate the world are typically LLMs (Large Language Models) such as ChatGPT.	Wall, 2018
ARPANET	ARPANET stands for Advanced Research Projects Agency Network. It is the world's first computer network and the precursor to the internet. First used in 1969, it is mainly used for the scientific and academic research community.	Abbate, 1999; Leiner, 1997
BITCOIN	Bitcoin is a type of cryptocurrency, invented by Satoshi Nakamoto in 2008 when he punished his infamous whitepaper on the topic. Bitcoin allows for digital transactions through peer-to-peer electronic payments which are decentralized, pseudonymous, and use blockchain technology to create digital ledger of chronologically ordered activities.	Nakamoto, 2008
BLOCKCHAIN	Blockchain is the digitally distributed and decentralized ledger of transactions. It is the technology that tracks the activity each transaction for most cryptocurrencies. The blockchain technology makes it so cryptocurrency transactions are transparent so they can be tracked while also being pseudonymous as they do not contain any personal information, just identifiers.	Nakamoto, 2008; Tambe and Jain, 2024
CLOUD COMPUTING	Cloud Computing refers to data storage, computer power, and platforms that enable remote data storage and access through the internet as opposed to directly on an individual device. If your files are 'in the cloud', they are being stored in a large data centre as opposed to directly on your device.	Wall, 2018
CRYPTO COINS	Crypto coins run on their own blockchain and have a set value. Usually, cryptocurrency is a term that refers to crypto coins.	Hicks and Adams, 2024
CRYPTO RANSOMWARE	Crypto ransomware encrypts the data so that even if the malware is removed or storage is moved to another device, the data is inaccessible.	Richardson and North, 2017
CRYPTO TOKENS	Crypto tokens are another form of digital currency or digital value. A token represents a digital asset or utility stored on a blockchain database, but each token may have a unique value.	Hicks and Adams, 2024

CRYPTOCURRENCY	Cryptocurrency is digital currency which is usually decentralized, secure, and pseudonymous. Many cryptocurrencies use cryptography to secure and encrypt transactions. The decentralized nature means that cryptocurrency transactions are direct, do not require a third party, and are not monitored or regulated by any centralized banking entity.	Hicks and Adams, 2024
CRYPTOGRAPHY	Cryptography is a process of coding information so that can only be read or understood by those with the correct keys.	Nakamoto, 2008; Tambe and Jain, 2024
CSSF	Conflict, Stability and Security Fund (United Kingdom)	
CYBERCRIME	Cybercrime is crime committed by means of or using the internet or computers.	Sukhai, 2004
DARKNET	The darknet is also frequently called the dark web. It is a part of the internet which is not accessible or visible to the public through regulated search engines and browsers such a Safari, Google, or Chrome. Instead, the collection of sites on the darknet are concealed through software that anonymises their IP addresses. The sites on the darknet are typically discussion forums, marketplaces, or websites for particularly groups or organizations (e.g., ransomware group pages).	Minnaar and Reddy, 2018
DDOS	DDoS stands for Distributed Denial of Service. It is a type of DoS (Denial of Service) attack which makes a network, software, server, or machine unavailable or unusable. It works by disrupting the targeted with an overwhelming amount of internet traffic or activity.	Porcedda and Wall, 2019
DOD	Department of Defense (United State)	
DOS	DoS stands for Denial of Service. It is a type of cyber-attack that overwhelms a server, network, or device by flooding it with excessive amounts of activity or traffic.	Porcedda and Wall, 2019
ENCRYPTION	Encryption is a mathematic process of computationally securing or coding information such that it cannot be understood or accessed in a meaningful way without a key.	Minnaar and Reddy, 2018
ETHEREUM	A popular cryptocurrency.	Hicks and Adams, 2024
FBI	Federal Bureau of Investigation (United State)	
GDPR	General Data Protection Regulation (European Union)	
IMF	International Monetary Fund	
IOT	IoT stands for Internet of Things and it is a category of objects or devices that are embedded with monitors, sensors, or other software that allows them to connect with other devices or the internet.	Wall, 2018
LLM	LLM stands for Large Language Models. Large Language Models fall under the general category of AI.	

	They generate text and content through computational and statistical calculations based on large sets of data.	
LOCKER RANSOMWARE	Locker ransomware simply locks the data on a device.	Richardson and North, 2017
MALWARE	Malware is literally “malicious software” and encompasses different form of malicious software such as viruses, worms, trojan horses, ransomware, spyware, etc.	Loebenberger and Wielputz, 2006
NHTCU	Netherlands National High Tech Crime Unit	
RANSOMWARE	Ransomware is a type of malware attack which usually prevents victims from accessing their data by encrypting and or stealing it. Attackers perform this data-based extortion by requiring victims to pay, usually in cryptocurrency, in order to recover their data or files.	Richardson and North, 2017
SQL	SQL stands for Structured Query Language. It is a programming language for data and database management.	Porcedda and Wall, 2019
TCP/IP	TCP/IP stands for Transmission Control Protocol/Internet Protocol. It is the network protocol or organizational framework for network communication for the modern internet.	Leiner, 1997
TOR	Tor stands for “The Onion Router”, and it is the anonymous network for much of the darknet. Tor is built on open source, encrypted software and allows users hide their identity and activity.	Bearman, 2020a
USD	United States Dollar	
WWW	WWW stands for World Wide Web. It is the information and content sharing system for the internet.	Loebenberger and Wielputz, 2006