Journal of Law and Criminal Justice
December 2020, Vol. 8, No. 2, pp. 67-79
ISSN: 2374-2674(Print), 2374-2682(Online)
Copyright © The Author(s). All Rights Reserved.
Published by American Research Institute for Policy Development
DOI: 10.15640/jlcj.v8n2a5
URL: https://doi.org/10.15640/jlcj.v8n2a5

White-Collar Cybercrime: Evaluating the Redefinition of a Criminological Artifact

Christopher Hamerton[1]

Abstract

This paper explores the cause and effect of cybercrime from the perspective of what has been termed white-collar cybercrime, providing a layered analysis of established theoretical models and typologies and evaluating these to determine where white-collar cybercrime might fit within the evolving discipline of cybercriminology and wider interdisciplinary social sphere. White-collar crime itself offers the rare example of a criminological theory that has the attributes of an artifact - establishing a distinct criminal offence type within law and criminal justice and entering mainstream knowledge and terminology within half a century of inception. Despite this, white-collar cybercrime is a relatively new concept for cyber criminological analysis and is currently a rarity within the academic literature. Thus, the piece primarily seeks to compliment and expand recent scholarship in offering further critical evaluation of an important emergent model. This is done in terms of its history, evolution, characteristics, position within social change theory, and via examination of some of the many policy, practice and security challenges that appear inherent to the modern networked workplace.

1. Introduction

The earliest criminological conceptions and explanations of computer crime - with machine operated to facilitate offence – perceived the model as belonging to the then still developing sub-category of "White-Collar Crime". Indeed, Donn Parker's early pioneering work in this area saw the computer, to a large extent, as related if somewhat peripheral to the well-placed offender, but key to the offence - a technical tool or device to facilitate individual dishonesty (Parker, 1976; 1980, 1983). In the early years of computer crime this already familiar, but still provocative, terminology provided a convenient focus for these technical offenders, able to hide behind the complexity of new science. At this point, in the social sciences and security industries at least, the creation and growth of the World Wide Web could not have been conceived outside of science fiction.

The personal computer revolution of the 1980s which became turbocharged by the creation of the internet and browser technology in the 1990s ensured that computer crime has become a global social problem affecting almost all countries since the onset of the Millennium. The socio-political activity that has enveloped computer crime often depicts it as an overwhelming problem worldwide, conveying an array of new crime activities and actors and, consequently, a series of new challenges in the fight against this new threat (Wall, 2007; Jaishankar, 2007; Picard, 2009; Holt and Bossler, 2016; Holt et al., 2017; Yar and Steinmetz, 2019). The construction of a security bulwark which attempts to 'police' computer crime is a knowledge-intensive challenge indeed, because of the innovative and adaptive aspects of the genre. Thus, even two decades into the 21st century cyberspace continues to appear as a moveable feast, continually evolving to present challenging new frontiers for criminology, police science, law enforcement, public policing, the private security sector and policy strategists.

Fundamentally, the proliferation of information communication technology (ICT), virtual reality, computer-mediated communications and the growing establishment of artificial intelligence (AI) has directly challenged the traditional discourse of criminology and the reactive police work informed by it, regularly introducing new forms of deviance, crime, and social control. Since the 1990s, a growing phalanx of academics and practitioners has observed how cyberspace has emerged as a new field of criminal activity. It can be argued that cyberspace has fundamentally changed the nature and scope of offending and victimisation. In response, the new sub-field of "Cybercrime" emerged as the study of crimes that occur in the virtual domain hat can impact in the physical world. Such causation and impact continues to transform, proliferate, and ultimately inform the field.

[1] School of Economic, Social and Political Sciences, University of Southampton, University Road, Southampton SO17 IBJ, United Kingdom. Email: c.t.hamerton@soton.ac.uk.

Edwin Sutherland (1939) in providing the initiating and enduring terminology of White-Collar Crime later recognised his concept as fluid, ambiguous, and necessarily developmental, a point emphasised by David O. Friedrichs in his 2009 pitch for a reconfiguration towards what he termed "technocrime" arguing that "the problem of crimes committed in cyberspace will increase in the future and will increasingly be a key element of different forms of white-collar crime" (Friedrichs, 2009: 217). However, a decade on from Friedrich's rallying call the concept remains a rarity within the criminological literature, and no single large-scale work has addressed the subject as a discrete phenomenon. This critical review article aims to contribute towards plugging the theoretical gap, as an addition and compliment to a cluster of thought-provoking recent scholarship that has provided stimulus within the paradigm (Graves et al., 2019; Hutchings and Collier, 2019; Payne, 2018; Isenring et al., 2016). Thus, its *rationale* is to augment the current literature on cybercrime, by examining the proliferation whilst paying particular focus to its founding category within criminology; the currently under-researched concept of white-collar computer crime, latterly cybercrime, and subsequently white-collar cybercrime. This is done by recognition of the strong lineage and correlation that exists between the study of white-collar crime and cybercrime, with attention given to the points of convergence, as well as the points of divergence that have developed as computer technology and cybercriminology has come of age during the past three decades. The primary focus of the piece in terms of theoretical perspective, experience, and policy is the United Kingdom, specifically England and Wales, but where appropriate a comparative analysis is offered which draws on primarily American, concepts and models, particularly with regard to white-collar crime. This is done to determine where white-collar crime exists within the online contemporary workplace and how this might relate to the ongoing discourse on cybercrime.

2. White-Collar Cybercrime: Evolutionary Definitions and Characteristics

Analyses of contemporary white-collar offending often commence with a series of competing and occasionally contested definitions, a situation potentially rendered yet more complex still by the addition of a cybercrime suffix - but worthy of critical scrutiny nonetheless. Such contestation is to be expected to an extent, due to the pace of social change in terms of commercial activity, organisational behaviour, workplace culture, and global focus– crucially the way business is done and money is now moved – in the eight decades that have passed since Sutherland launched his hypothesis. However, testament to its success and endurance as a *tenet* can be seen in that it now appears well within the mainstream, with 'white-collar crime' established and recognised as common terminology well beyond the realm of academia. This current acceptance should not screen or obscure the level of controversy attached to Sutherland's work in his time, with the theory, first delivered in his presidential address to the annual meeting of the American Sociological Society in 1939, received by many contemporaries as a direct afront to the competitive spirit of the capitalist ideal. A decade on he reflected that his white-collar crime theory:

> "stated positively, is that persons of the upper socio-economic class engage in much criminal behaviour…These violations of law by persons in the upper socio-economic class are, for convenience called 'white-collar crimes. This concept is not intended to be definitive, but merely to call attention to crimes which are not ordinarily included within the scope of criminology. White-collar crime may be defined approximately as a crime committed by a person of respectability and high social status in the course of his occupation" (Sutherland, 1949: 9-10).

Clearly, Sutherland was aware that his methodology would need to be reinterpreted as necessarily flexible and evolutionary. Allowing for redefinition and open to structural change to confer longevity but with the core value that the crimes committed by the middle classes should be regarded as being 'real' crime, holding the potential to cause real social harm. Though clearly aimed at inclusivity, this theoretical flexibility has encouraged dispute and ambiguity, with adapted models variously designated as *inter alia* business crime, financial crime, commercial crime, organisational crime, workplace crime, occupational crime, elite deviance, and corporate crime emerging, and often competing, under the white-collar crime umbrella since. Leaving Friedrichs to persuasively argue "perhaps no other area of criminological theory has been more plagued by conceptual confusion than that of white-collar crime" (Friedrichs, 2002: 243).

In terms of applicability to computer crime, and subsequently cybercrime, perhaps the most persuasive classic interpretation was that provided by Clinard and Quinney in their examination of *Criminal Behaviour Systems* (Clinard and Quinney, 1973). Here, they split white-collar crime into two forms, differentiating between corporate crime (an emerging theoretical development at the time)[2] as a group offence where the body corporate is the intended investor and beneficiary of the criminal action; and occupational crime (a variable much closer to Sutherland's original concept), defined as an individual offence where the criminal activity is designed to benefit

[2] Clinard would later clarify corporate crime as "illegal corporate behaviour, which is a form of collective rule breaking in order to achieve organizational goals"(Clinard, 1983: 17).

The individual actor. In this delineated definition individual employees on a frolic of their own in terms of criminal behaviour in the workplace are seen to be committing offences for themselves in the course of their occupations to the detriment of their employers. This would appear to offer an appropriate fit and model for the early interpretations of what was deemed "white-collar computer crime", with the imagined offender sited in the workplace in front of the keyboard of their Personal "Micro" Computer with access to sensitive information, or worse still, in possession of the specialist knowledge of how to obtain it.

Parker, arguably the leading scholar on computer crime throughout the 1960s into the 1980s, at that time referenced this behaviour as "Computer-Related White-Collar Crime" a *modus operandi* appellation. Revisiting this fascinating initiating work now much of his analysis appears visionary, covering many of the behaviours which might now fit as a definition of contemporary white-collar cybercrime: -fraud; embezzlement; theft; extortion; sabotage; and conspiracy - but also predicting the inherent difficulties in detecting, measuring, and prosecuting such offences, and the urgent need to expand criminology and criminal justice to incorporate the coming technological impact. Moreover, Parker predicted that this significant growth was obvious with the proliferation of computers occurring in sensitive areas of business and other key societal functions, and the increasing positions of trust occupied by skilled data processing professionals within organisations. The focus at this time was primarily on stored static data, but as is pointed out, though the number of potential offenders was small, the assets that might be plundered were huge (Parker, 1980). Similarly, Willis, writing in 1986, saw computer crime as clearly belonging to the white-collar crime genre, his contemporary exploration provides a valuable barometer of scale and seriousness at that time:

"The introduction of fast, inexpensive microcomputers is one of the most important phenomena of our time. Along with giving managers instant access to information and making their jobs easier, it has made it relatively easy for a skilled bandit or dishonest employee with a personal computer and a modem to obtain confidential data – or millions of dollars – from unwitting companies, banks, and government agencies. In 1978, there were at least two million Americans with access to computer systems: there are probably two or three times that number today. Losses to computer crime have been estimated by the Department of Justice as at least $100 million annually, not counting the costs of investigation and prosecution" (Willis, 1986: 26).

The sense is one of a burgeoning crisis in terms of technology dictating the pace of social change whilst potentially outflanking social norms, institutions and existing laws. This sense of sudden expansion is also evident in the work of Molnar (1987), which focused on putting computer-related crime in perspective in terms of public policy. Noting that the terms "hacker" and that the threat of sophisticated computer-related crime were being readily embraced by politicians, media, Hollywood and the general public,[3] he too situates the phenomenon as a new form of white-collar crime, whilst highlighting its misrepresentative sophistication by reference to its increasing ordinariness:

"in reality, most computer-related crime is far from high tech; it is a crime of the common man. Available evidence shows most computer-related crime is committed by clerical, case/claim review, or client services employees. Their *modus operandi* is simply to alter data in the computer system, either while handling input documents or while sitting at an online terminal. They do this as if it were a normal part of their job…they are nonsupervisory, nonmanagerial, nontechnical employees. Very few cases of computer-related crime involve in-house computer personnel; even fewer involve external high-tech criminals" (Molnar, 1987: 714).

According to Molnar, this low-level menace would likely be controlled via effective managerial control measures and systems within organisations, through checks and balances, audits, reviews, and improved employee surveillance allied to the threat of discovery, dismissal and prosecution. Interestingly there is a clear consensus as to where this new type of computer offender sits in terms of criminology and the criminal justice process - squarely within the parish of white-collar crime - regardless of career seniority or skillset, seated at a computer terminal the collar can be both white or off-white.

Knowledge of this early history of personal computer use appears useful, and potentially persuasive, in terms of contemplating how white-collar computer / cyber criminals might be conceived in the present. Applying Clinard and Quinney's concept of the white-collar criminal to an individual, offending within their normal occupational routine or site for their own benefit, appears to chime with the model of the computer-related white-collar criminal favoured by Parker. This is also a wide enough definition to include Willis's motivated managers and Molnar's mundane clerks.

[3] Molnar specifically refers to a trio of fanciful computer-crimes depicted in contemporary movies, the "salami attack" in Superman III, the "trap door" in War Games, and the "logic bombs" in The Intruder. All feature and develop the motivated skilled lone offender architype.

Moreover, despite the obvious changes in technology and working practices as well as potential overlap with current models of cybercrime – *individual actor; in the workplace, offending for their own benefit*– is also a model that might be considered within the present.

Recent research supports the hypothesis that individual employees within organisations commit a majority of what might be termed financial computer crime against their employers, and that this criminal activity usually occurs within the walls of the host company (Gottschalk and Gunnesdal, 2019; Hutchings and Collier, 2019; Nurse et al., 2014; Hagen et al., 2008; Levi, 2008; Nykodym et al, 2005; Dhillon, 2001; Hamin, 2000). Moreover, this would allow a nuanced perspective which redefines white-collar computer crime (latterly cybercrime) to incorporate a consideration and profit-oriented crime, alongside the familiar interpretation of damage-oriented crime, thereby moderating the conventional focus within cyber criminology of disgruntled employees simply wanting to humiliate, sabotage or frustrate their employers. Profit in this sense could be defined broadly, encompassing financial gain of course, but also considering autonomy, personal advantage, benefit, and gratification.

2.1. Delineating Social Change and Social problem: Computer-crime to cybercrime

The characteristics of computer-crime as we currently understand them have been framed by the vigorous development of the World Wide Web. Over little more than a generation its cascade of effects on globalised society and the associated emergence of what has become widely known and accepted as cybercrime as a consequence. The internet appears for many under the age of 30 as an immutable social fact, attaching itself to most if not all aspects of contemporary social life – work, rest, and play – and is now best analysed as an integrated entity rather than a limb with separate cyber appendages.

What is now known as the Computer Revolution started in the 1970s with the advent of microprocessor and microcontroller technologies, and by the middle of the decade increasingly powerful single silicon chips could be found in readily available consumer goods, such as pocket calculators and digital watches. This was followed by the microcomputer, originally promoted towards small and medium sized enterprises (SMEs) as a labour-saving device on lease or hire purchase, to aid in day-to-day accounting practices, word processing and database management. By the early 1980s microcomputing had crossed-over into the domestic market with many households using the machines for both home-office and leisure activities.

As microcomputer technology developed and began to become familiar in the workplaces and homes of the middle classes in developed countries, advances in semiconductor and optical technology led to the viability of a commercial public communication network; an *internet,* with the first Internet Service Providers (ISPs) appearing in 1989. and the first web browser designed by Tim Berners-Lee, a researcher at CERN,[4] appearing the year after which he named "WorldWideWeb". Following Berners-Lee's decision to release the browser outside of CERN in 1991 the popular use of the World Wide Web gathered pace, initially via a system called *Mosaic* which was quickly overtaken by the now familiar *Netscape Navigator* and *Microsoft Explorer* browsers enabling the Information Age (Castells, 1996; 2002). Since this critical point in the mid-1990s the internet has grown exponentially year upon year, to the point where it dominates the global spheres of economy, social life, and culture. The latest combined statistics from January 2020 are both remarkable and illuminating: with currently a world population of 7.75 billion (up from 7.67 billion in 2019) which includes 5.19 billion unique mobile phone users (up from 5.11 billion in 2019); 4.54 billion internet users (up from 4.38 billion in 2019), and; 3.8 billion active social media users (up from 3.48 billion in 2019).[5] Such proliferation comes with what Tim Berners Lee recently described as the "roses and thorns" natural to his invention[6] - the light with the dark, the good with the bad, opportunity and risk, concord and conflict - the dichotomy of cybervirtue and cybercrime.

The notion that internet use carried inherent risk was discovered very quickly, moving from the parochial practice of computer-crime which primarily targeted static databases to the globalised ability to target, breach and access live networks. This transfer towards Information Technology (IT) crime was described by Thomas and Loader in the following terms "Computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global networks" (Thomas and Loader, 2000: 3) – it was the *network* element that provided both the impetus and stimulus, essentially weaponising computer-crime.

[4] Conseil Européen pour la Recherche Nucléaire, Geneva, Switzerland.

[5] Digital Global Overview Reports, 2019 and 2020, (Sources: United Nations, Local and Regional Government data, GlobalWebIndex, Statista, GSMA Intelligence, App Annie, SimilarWeb, Locowise) [Online] Available: https://wearesocial.com/digital-2020 (September 26, 2020).

[6] Sir Tim Berners-Lee (2019). The World Wide Web: A Mid-Course Correction. The Richard Dimbleby Lecture, UK: BBC Television [Online] Available: https://www.youtube.com/watch?v=CmcIVdtVvJw (September 12, 2020).

The amalgam term "Cybercrime" first appears at around this juncture, created by the team responsible for drafting the Council of Europe's Convention on internet Crime in 2000, which appeared as the Budapest Convention on Cybercrime in 2001.

Cybercrime has since developed as a catch all term used to describe the use of cyberspace to commit a crime, encompassing a wide range of deviant and criminal behaviours that are facilitated by computer technology. These vary between what might be summarised as: i. Crimes *against* the machine (hacking and cracking, paralysing computer networks; Denial of Service attacks; ii. Crimes *using* the machine (deception, fraud, theft, extortion, embezzlement), and; iii. Crimes *in* the machine/on-screen (grooming, obscenity, stalking, hate speech). However, the subject itself is often construed and applied narrowly and rarely considered in terms of wider social theory or indeed where it might fit historically, despite important considerations that might go some way to explain why its effects have been felt so acutely in terms of public and political perception of fear and risk over the past thirty years. Populations in developed post-industrial societies, particular former industrial powerhouses, have tended to receive the rapid path towards globalisation as a form of social fragmentation and disintegration bringing with it an absence of moral parameters, a new and confusing age of uncertainty. In this sense both globalisation and the internet are partners in blame for releasing a set of risks that appear to threaten humanity, risks that have to be identified, prioritised, managed, and controlled (Beck, 1992). Within this tech induced maelstrom danger appears omnipresent "crime is no longer seen as an aberration but rather an everyday risk to be managed like air pollution and road traffic" (Garland, 1996: 4).

A fundamental starting point to glean a wider perspective might be provided via an exploration of social change theory, a concept that would also provide linkage to Sutherland's observation towards the necessary evolution of his white-collar crime thesis. Vitally, social change adds complexity to a society, complexity that requires an increasingly complex means of administration and social control, including technological drifts and shifts, a concept known as *Differentiation*. Such differentiation is made tangible by the crafting of social norms, social policy, and legislation. This can clearly be seen with regard to cyberspace with the construction of the World Wide Web appearing as vehicle for globalisation and neoliberalism, and participation in the project infrastructure viewed as a form of economic and cultural emancipation requiring a degree of compliance from participating states. However, as Roach-Anleu argues, technological advancement does not necessarily guarantee liberation, greater prosperity or security: "sociology as a distinct discipline was characterised by large scale economic, political, and social transformation. There is often an assumption, either implicit or explicit, that social change is tantamount to social progress" (Roach-Anleu, 2000: 2). Assumption can frequently lead to disappointment.

What has been delivered by this unprecedented period of techno-social change is a path from microchip technology to cybercrime policy in a single generation, a pathway bordered by roses and thorns, or concord and conflict, depending on your theoretical point of view. For some, cyberspace is intrinsically functional with cybersociety as biological organism seeking "homeostasis" for the benefit of the whole – social change is *evolutionary,* adaptation / integration enables techno "progress" which appears inevitable. For others, cyberspace is a site of struggle with conflict seen as the driving force behind revolutionary social change – here one might consider the globalised socio-political reaction to Wikileaks, Anonymous, Chinese and Russian State Hacking, online obscenity and cybercrime generally. However, history suggests that human momentum to an extent is irresistible regardless of how it is viewed, with social change occurring when there is a purposeful impetus for that change. For example, as Hobbs and Hamerton suggest with regard to innovative technological change as the contemporary driver of differentiation: "in the 1970s and 1980s, the invention of the personal computer and its proliferation in the workplace led to a need for computer literacy to be added to the school curriculum as education policy. A generation on, concerns over cybercrime have required consecutive governments to consider policy and legal changes to combat computer misuse" (Hobbs and Hamerton, 2014: 23).

The *ying and yang* of cyberspace, its intrinsic dichotomy, is that the social network creates social problems that necessitate social policy. Here, social problems might be described, in a broad sense, as undesirable behavior worthy of social action in the form of censure, policy or legislation. Consequently, government policy can provide a reasonably reliable barometer and conduit of the concerns and conflicts that exist in modern society. However, the concept of social problem is subjective and controversial with a majority imperative: "A social problem is whatever a significant part of the population perceives as an undesirable gap between social ideals and social realities and believes can be eliminated by collective action" (Robertson, 1980: 4). The overriding question that this poses in terms of cyberspace is whether cybercrime has been (or can be) challenged via consensus, and might be (or has been) arrested or purged by policy and legislation?

2.2 Characterising cybercrime as *the* social problem of our time

In order to evaluate where we are in terms of a recognised typology of cybercrimes or cybercriminality, its underlying character and form as a social problem must be considered. Such typological considerations are necessarily broad, and in this regard the following four headings are suggested, encompassing: *Cyber-Trespass; Cyber-Theft; Cyber-Obscenity*, and; *Cyber-Violence* - each variable theoretically capable of supporting white-collar offending online: *Cyber-Trespass:* hacking, malicious damage, defacement, virus release, blackmail, denial of service attacks, and attacks on electronic control systems. Offences founded on crossing virtual boundaries to cause damage, with hacking construed as providing the breaking and entering which facilitates unauthorised access to a computer, system, or network. Deviance and crime within this category potentially range from pranking and spoofing, and vandalism and voyeurism to intimidation, sabotage and terrorism; *Cyber-Theft:* credit theft, identity theft, credit card fraud, media piracy, industrial espionage, money laundering, advanced fee fraud (419 cases), phishing. Offences based on theft, deception or extortion (or attempts at theft, deception or extortion) via utilisation of the internet. This category would include both individual white-collar crimes and large-scale group organised attacks, with goals ranging from the theft of money or / and information, the commission of fraud and the appropriation of real, electronic or intellectual property to internet piracy; *Cyber-Obscenity*: obscenity and indecency violations, the transmission and sale of restricted, harmful and illegal materials including violent abuse imagery, child pornography, voyeurism, and articles which facilitate hate speech. Offences within this category are often categorised and posited as familiar offences revitalised by a new medium, covering both individual offenders (where the primary motivation is often self-gratification) and group / organised offenders (where the motivation might lie in group acceptance or protection and / or financial gain). This category, loaded with socio-cultural and legislative variations, provides the most problematic and active area in terms of a globalised approach towards universal policy and legal plurality. However, despite what seems a continuous drive towards universalism the conundrum remains as to what should collectively be considered obscene, indecent or offensive in a borderless, globalised cyberspace. *Cyber-Violence*: psychological harm, inciting physical violence, inciting racial or religious hatred, cyberbullying, cyberstalking, revenge pornography, attempts at the exertion of power or control over the victim. Offences founded on the infliction of psychological harm and / or the incitement of physical harm. In terms of behaviour this definition might include the sending or public display of abusive, unwarranted, unsolicited, threatening or offensive materials online against the knowledge, wishes, or will of the victim, likely to cause distress, alarm, or fear. In many cases within this category the effect of the internet has been to act as an amplification device, an enveloping mediated means of increased, potentially around-the-clock torment, resulting in an intensified form of victimisation.

A perceived surge of novel cyber induced social problems has been met by an accompanying wave of social policy activity. This has led to a number of studies within cyber criminology reflecting on the concept of "old wine in new bottles" – these consider whether cybercrime is a *new type* of crime, or simply a *new way* of committing old crimes? Again, a question that adds pertinence of current examinations of what might constitute white-collar crime in the digital age. Perhaps the most sophisticated treatment of this issue has come from Michael McGuire in his book *Technology, Crime and Justice* (2011). This book introduces what McGuire terms "Technomia" a concept derived from Berger's (1967) call for "nomos" described as "the body of rules, codes and formal or informal regulations that governs a social practice" (McGuire, 2011: 27). Here, it is suggested that the contemporary nomos of technology should be *technomia* (the regulatory ordering of technology). This links well with the foregoing examination of how rapid social change (driven by technology) can create perceived social problems and then generate a new nomenclature for these, whilst requesting and seeking social policy and legislative interventions to address these "new" threats. Maguire argues that technomia (contemporary technology) is received and organised around three questions, abridged and summarised here as: How is technology regulated in terms of which regulatory structures contain it?; Under what conditions are these regulatory structures seen to be violated and at what point does this violation constitute a criminal offence?; What are the kinds of ways in which the technology itself acts as a regulator and is there blurring between technical and legal control?

Considering such questions might lead us to reflect that in reality technology and crime have always gone hand in hand, with the invention of currency requiring the invention of the purse and leading to the pickpocket, livestock owner to poacher and rustler, the safe to the safecracker, the car to the car-thief, the telephone to the phone-phreaker, the computer to the computer hacker, and so on – social change allied to technology creates social problems, with yet further technology and differentiation key to how these are received and perceived by society.

Thus, the concept of technomia offers real scope as to how we might define our collective experience of cyberspace in terms of delineating between old wine in new bottles, or at least consider the value of a vintage appellation over a recent novelty or how quickly it is being served to us. Perhaps white-collar crime is a good enough label for white-collar computer offences or is it a question of what happens (the type of offence) or where it happens (offline or online) in the eyes of the Criminal Justice System?

It can certainly be said that cyberspace has provided stimulus and added layers of variety to the criminological subject. But in doing so it has also conferred a great deal of complexity on the criminal justice process with many cases which possess cyber elements requiring additional expert case analysis in terms of process, Brenner and Koops clarify: "is it the place of the act, the country of residence of the perpetrator, the location of the effect, or the nationality of the owner of the computer that is under attack? Or all these at once?" (Brenner and Koops, 2004: 3). In response many governments have developed hybrid policy models that work on the basis of a legal paradox of stability and fluidity, whilst keeping a watching brief towards the need for defined cyber policy, the crossover from the real to the fully virtual offence. This is evident in the work of Neal (2010), who offers an innovative pragmatic model that incorporates both the established and the new, with space for crossover in-between. This is based on three interrelated classifications that she identifies as *Traditional cybercrime; Hybrid cybercrime* and *True cybercrime*, which follow in here: 1. *Traditional cybercrime* relates to immediately recognisable criminal behaviors with which the criminal justice system is familiar and which it regularly encounters; 2. *Hybrid cybercrime.* This category refers to those criminal activities that, like 'traditional cybercrime', can also behaviors and activities that can exist 'offline', and; 3. *True cybercrime.* This category refers to those criminal behaviors that are wholly contained within and by cyberspace (Neal, 2010: 77).

Considering the typology and character of contemporary white-collar cybercrime in particular, it can be argued that the genre incorporates analogous processes common to a number of other types of crime that appear as emblematic for cybercrime generally. Typical examples that employ comparable and often complex techniques are hacking and cracking, online grooming of specific targets, and sharp practice in accessing illicit or restricted information. Fundamentally the characteristics of motivated and technically sophisticated offenders who are capable of committing or commissioning complicated and frequently obscured offences. To argue for the "white-collar" designation workplace and / or course of occupation appear as the key distinguishing variables, with the traditional sites used for analysis of white-collar offending and internal misconduct, such as the banking industry, the financial services sector and police departments well represented in case law. Within Neal's categorisation potential for what might be described seen as white-collar cybercrime could be identified within all three of her discrete categories, and in certain cases within all the elements of an individual offence – such as the employee hacker sat at her office desk who virtually breaks and enters to steal online and then sells via contact with traditional fences. Such classification can also be seen in terms of official criminal justice policy within the United Kingdom, particularly when considering prosecution guidelines and policing strategy.

3. Public and Private Security Response to Crime in the networked workplace

The UK Crown Prosecution Service (CPS) currently distinguishes between two crime types which form important pillars of the government's National Cyber Security Strategy 2016-2021. These in effect refine the groupings in the foregoing, distinguishing between: *Cyber-dependent crimes*, these being crimes that can be committed only through the use of Information and Communications Technology devices, where the devices are both the tool for committing the crime, and the target of the crime, and; *Cyber-enabled crimes,* traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (CPS, 2020)[7] - once again the prosecution of a white-collar cybercriminal would feasibly straddle both categories.

The Public policing response to cybercrime in the UK, in tandem with many other public bodies, has been to identify cybercrime as worthy of exceptional consideration, leading to the rise of the specialists. This resulted in the formation of the National Hi-Tech Crime Unit (NHTCU) in 2001 following lobbying from Chief Police Officers who were concerned over the rising tide of computer and internet crime, in particularly fraud and obscenity. However, soon after formation it became apparent that the challenges faced in the new millennium were structural and global rather than caused by a lack of jurisdictional specialism. Cybercrime quickly became seen as an ambiguous term, allowing for a slippery theoretical framework which hampered the design of exact policy, legislative, and tactical response. In particular it became clear that many cybercrimes were too small in impact to be reported or prosecuted successfully, that existing law did not adequately cover every form of computer or online offence – with no law equating to no crime.

[7] Crown Prosecution Service (2020). Cybercrime Prosecution Guidance, London: CPS [Online] Available: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (22 September, 2020).

Proving causation and collecting evidence was also seen as problematic as was knowing who, where and how to prosecute. Moreover, cybercrime was going undetected and was not being followed up by the police in terms of routine operations. Furthermore, cybercrime was frequently unreported, often due to victim embarrassment that it was deemed not serious enough to contact the police, or in the case of white-collar cybercrime involving employees, corporate embarrassment of exposing security weakness at the cost of public trust (Gioia, 1996). By 2007, Wall estimated that only 10% of computer related crime was being reported and less than 2% of cases resulted in prosecution (Wall, 2007).

Soon after the formation of the NHTCU Jewkes acknowledged that the scale of the task at hand facing the police was virtually unassailable due to the sheer size and scope of the internet, placing the police in a spiral of catch-up (Jewkes, 2003: 502). By 2006 the NHTCU had been subsumed into a much larger unit The Serious and Organised Crime Agency (SOCA), which was created under the Serious Organised Crime and Police Act 2005 as the "British FBI" incorporating a range of specialist civilian investigators such as accountants, financial analysts and computer experts.[8] This incarnation would last for a further seven years when it was incorporated into a yet larger National Crime Agency (NCA), further refining national specialism for cybercrime threat and acting as a contact point for international agencies, such as Interpol and Europol. Reinvention, specialisation and the cyber arms-race have become *motifs* for cyber policing, with the aid of an ever-growing emphasis on public / corporate responsibilation and the assimilation of the private security sector.

3.1 The Key Role of Trust within the Amplification Spiral of the Internet

With a constantly expanding virtual frontier that has remained open and relatively free of state content control for three decades trust can be identified as key in terms of online conduct and control. Indeed, within many cyber spheres the actions and reactions of private (non state) actors, organisations and committees appear essential to "policing" the internet in its current form. This allows the reinforcement of the "private" and "free" counter-cultural ethos of cyberspace whilst reinforcing responsible norms and standards, self-control and regulation - responsibilisation. It can be argued that internet culture favours self-regulation in a space of predominantly open communication free from state censorship and intervention, what Castells referred to as the "bottom up" culture of the internet, with users / stakeholders as its lifeblood and inbuilt control mechanism (Castells, 2002), a situation that enables social harmony rather than social control.

Over the last decade, increasingly active online citizenship (netizenship) and political pressure has resulted in the creation of systems of social control and sanctions by user communities to report and address deviant behaviours, particularly in terms of freedom of expression and social media use. However, meeting the socio-technical challenges of cyberspace and to a large extent cyber deviance and crime is still retained as a mostly amateur pastime, albeit increasingly in tandem with Internet Service Providers and Regulators. At the present time public voice, scrutiny, and essentially consumer power, are still recognised as holding immense sway online, with information, exaggeration and misinformation able to quickly generate and galvanise social media campaigns which influence and lobby, particularly in cases which involve political scandal, corporate wrongdoing or breach of trust.

The importance of trust and reputation is acutely felt in the business sphere where the advent of the World Wide Web and the social discovery of cybercrime positioned the notion of institutional security as a borderless issue. Thus, bringing about the necessity of effective and tangible corporate security to safeguard assets and reputation within a global marketplace. This development has greatly extended the prospective damage of internal white-collar crime, with the potential reputational harm caused to private corporations and public institutions magnified by the mass amplification effect of the internet. For example, in the sphere of modern banking if an organisation were to be exposed as a vehicle for money laundering or not reporting suspected illegality in terms of transactions, its reputation would be seriously compromised. Negative publicity would likely result in both damage to reputation and tangible financial loss. Such organisations are fundamentally built on trust, and trust is explicitly linked to public perception - reputation is everything (Fukuyama, 1996; Braithwaite, 1989).

Reputation can be *everything* because reputational damage is often linked to a perceived weakening of a bank or professional service provider's financial soundness (Harvey and Lau, 2009: 59). The immediate manifestation of such damage is likely to be through the actions of account holders moving to withdraw funds and counterparties, sensitive to risk, withdrawing credit. Such a series of events could effect shareholder support and impact share price.

[8] Editorial. (2004). "Blair Unveils Plans for British FBI". Guardian Monday 9 February 2004, London [Online] Available: https://www.theguardian.com/uk/2004/feb/09/ukcrime.immigrationpolicy (14 September 2020).

Consequently, and particularly within the financial services industries, the significant cost associated with continually updating advanced internal and external cybersecurity measures to comply with regulations and standards is justified by the perception that breach or non-compliance will damage reputation and effect future business, even if the involvement of the institution is shown to be unintentional or technologically naïve (Johannes-Rose, 2020; Kshetri, 2013). Thus, in the borderless online business environment the potential for damage to corporate reputation by white-collar offending is exponentially increased, with consequences amplified and the former position of trust likely irretrievable. The effect of doing business, particularly international business, in the age of the World Wide Web is one of potential amplification – of both opportunity and ignominy.

3.2 Inside the firewall: White-collar cybercrime and organisational response

Echoing the activity seen in public policing since the mid-1990s the corporate and institutional security response to the perceived threat of both internal and external cybercrime has been to seek specialism and participate in a virtual "arms race" specifically in terms of *knowledge Management, intelligence* and *investigation*, a concise critical summary follows.

Knowledge management can refer to the systematic process of coordinating knowledge sharing and development to reach organisational goals - such as a drive to enhance corporate reputation or garner trustworthiness in terms of the public face. It usually encompasses Board and senior managerial efforts in attaining, producing, storing, diffusing, developing, and deploying knowledge by and from individuals and groups within the organisation. Knowledge management practices have to dovetail with the wider organisational context in order to be fully effective. They also need to be context specific, so that practice is able to influence organisational effectiveness, particularly when precipitating system weaknesses, employee deviance and possible criminality (Ratten, 2019). Zheng et al. explored the possible mediating role of knowledge management in terms of the relationship between organisational culture, structure, strategy, and corporate effectiveness. Advocating that knowledge management is able to fully mediate the impact of organisational culture on organisational effectiveness, and partially mediate the impact of organisational structure and strategy on organisational effectiveness (Zheng et al., 2010). Moreover, Hinduja posited that managing and employing knowledge gleaned from past experiences in terms of future planning can improve internal cybercrime investigations (Hinduja, 2007). Within public policing the near constant evolution of cybercrime has required police officers and prosecutors, generally, and those occupying specialist investigatory roles in particular, to allocate an increasing amount of their time towards technological knowledge management in order to positively identify individuals, events and causative processes to aid in the prosecution of offenders. However, within some corporations, knowledge management can be compromised by the frequently subjective and novel nature of cyber offending, a scenario intensified when committed or commissioned by a staff member recognised as possessing high value to the organisation. This may in turn result in lapses being dealt with in-house, by way of an internal closed compliance process. Such internalised practices possesses the capability to compromise trust and greatly harm reputation if socially discovered or revealed externally, (Isenring et al., 2016; Gioia, 1992).

The primary foundation of strategic business *intelligence* is the gathering of data and its close analysis to form the basis of response and action. As a cybercrime countermeasure an effective business intelligence process can enable an organisation to gain new insight into its security strengths and potential weaknesses. This allows key security decisions to be made in terms of adapting to internal and external cybercrime threats, often with the aim of strengthening public / consumer trust and / or enhancing (or repairing) reputation (Taken-Smith et al., 2019; McGee and Byington, 2013). The intelligence models currently favoured by complex organisations and large corporations have clear origins in public police science. Reflecting on this background, the customary policing process was primarily responsive, and based around covert information gathering on criminal behaviour. Contemporary models, however, habitually built around technology, tend towards the systematic, with intelligence collected and collated with the aim of tracking, predicting, assessing threat and allocating resources (Brown et al., 2004). Within the business context, specialists are employed to gather intelligence to investigate unusual or undesirable behaviour and explore cause and effect. Strategic recommendations can then be provided to tackle specifically identified threats or aid long term planning.

An overriding aim of intelligence strategy is to continue to develop intelligence led decision making in all parts of an organisation, institution or public body. Organisational intelligence strategy can act as a framework for structured problem solving and enable a partnership enhanced approach frequently based around a common purpose model. Ratcliffe regards this amalgam of intelligence-led policing and corporate strategy as *the* paradigm; providing both a "business model and a management philosophy" (Ratcliffe, 2008: 89).

Therein, effective intelligence strategy is seen to be adaptable and responsive – a nod to Sutherland's call for dexterity perhaps? – in order to counter and disrupt white-collar offending in the workplace, with a *holistic* approach to corporate / criminal intelligence likely to offer better adaptation to the exigences of emergent technocrimes (Barlatier, 2020).

Traditionally private workplace crime *investigations* have been highly dependent on internalised whistle blowing, a difficult and delicate process of peer detection likely drawing in board members, the chief executive officer, and senior management alongside internal security operatives (Peretz Glazer, 1996; Pickett and Pickett, 2002). Levi describes the nature of the public policing of financial crimes involving deception as focused on the management of risk within a complex environment, a setting still relatively enigmatic and inaccessible to address via routine policing methods. He states that: "policing frauds and other financial crimes creates particular financial and institutional difficulties because of the regularity with which such investigations cross jurisdictions, even at a fairly modest level of victimization" (Levi, 2007: 588).Here, with regard to the modern networked workplace, it can be argued that investigating / policing contemporary white-collar cybercrime is likely to include many of the traditional difficulties highlighted by Peretz Glazer, Pickett and Pickett as well as the jurisdictional challenges emphasised by Levi, in conjunction with surveillance and analysis of relevant online activities. When such cases occur, forensic cybercrime investigation can represent a costly and highly specialised field, fraught with difficulty in practice (Nurse et al, 2014; Callanan and Jones, 2009).Kao and Wang (2009) suggest that the adoption of a systematic and transparent model for undertaking cybercrime investigations is required for the workplace, this encompasses three principal areas: a) independent verification of digital clues; b) corresponding information from different sources, and; c) preparation of a valid argument. A methodical approach such as this is very necessary as *ad hoc* covert IT investigations of staff can represent a highly controversial practice when investigating financial crime, complicating, and potentially compromising recognised principles of evidence-based enquiry and infringing privacy rights at law (Koziarski and Lee, 2020; Tackett, 2008).

4. Conclusion

The business and popular press over the last decade on both sides of the Atlantic have consistently pointed to a resurgence of white-collar crime–often specifically intertwined with cybercrime – a popular recognition of *white-collar cybercrime* if you will (Healy and Serafeim, 2019; Ring, 2019; Henning, 2020; Katz and McIntosh, 2020; PwC, 2020). Whilst it is doubtful that such journalism is advocating or endorsing a terminological revival in criminological theory it does suggest that workplace computer enabled crime is on an upward trajectory, particularly relatively low to medium level offending, crimes that might benefit individual actors. Cues towards confirmation of the *newness* of this discrete form of crime may be premature, and it may be that the media, politicians and public are merely comfortable with familiar terminology - they are able to picture what "white-collar crime" looks like, and the "cyber" element is considered secondary – a reminder of the endurance of Sutherland's prototype and Parker's rational actor with a *device*, perhaps?

When considering the UK context in this regard, the reported increase in numbers may well be due to a number of structural factors. Amongst the most compelling tentatively would be over confidence and reliance on technical systems and countermeasures, allied to an increase in workplace disenfranchisement. In particular, palpable social strain with many businesses and the individuals who occupy them under a great deal of everyday pressure. For over a decade many people have been dealing with diminishing earnings and returns, shrinking markets and the growing precarity that has been in the background since the global crash in 2008 and its depressive financial aftermath. Traditionally, the undesirable bi-products of such periods of economic crisis have been identified as the heightened fear of disorder and an amplified perception of crime and deviance (Hall, et al., 1978).

Recently, in response to the ongoing Covid-19 Pandemic the *Times* of London ran a headline that announced "The World Economy is Now Collapsing" (Wolf, 2020). Not to be outdone two days later the *New York Times* declared "It's the End of the World Economy as We Know It" (Irwin, 2020). A genuine monumental change imposed by the Pandemic is that a majority of white-collar workers have found themselves having to adapt to "effective" online remote working, often government mandated, as the "new-normal" within the space of just a few months. In such circumstances how is the socially-distanced remote home worker in their isolated home office environment to be effectively managed? Which established workplace cyber security controls have been relaxed, sacrificed, or are no longer seen as operable? Can, should, or will organisations be able to monitor, surveil, or investigate employees working in the privacy of their own homes suspected of wrongdoing? Having to consider such questions seems inevitable within our current technomia. As this article has argued, rapid social change in terms of how technology is perceived and utilised is likely to produce both benefits and problems for what is a new phase of working life within the cyber sphere, and coupled with such bleak economic forecasts and impeded prospects incidences of white-collar cybercrime may well continue to rise.

The most recent official statistics in the UK suggest that whilst the number of reported computer-misuse and fraud cases grew in 2018/19 to 700,000 (a sizeable increase of around 107,000 cases from 2 014/15), the number of prosecutions for white-collar crime cases recorded for 2018/19 was 6,669, 1117 down on 2016/2017 and 2831 down on 2014/15 (Ames, 2019; Slingo, 2019). An aggravating reason for this is likely that the cuts to local police force budgets effecting critical resources (manpower and equipment) are being felt. With the investigatory scope of many police fraud teams reduced and constrained within the same period (Seifert &Mather, 2013; Mann et al., 2020). The constricted focus has necessarily moved away from small and medium localised offences towards large scale national operations targeting organised offenders. Meanwhile, cyberspace continues to develop and differentiate, and cybercrime within it. The concept of white-collar crime envisaged by Sutherland and developed by Clinard and Quinney to consider offences committed by individual employees offending in the course of their occupation for personal benefit offers an enduring model. Able to recognise and absorb social change and differentiation, allowing for layers of complexity and technology to emerge and for new crime types, victimologies, and policy responses to appear – the redefinition of a criminological artifact. "White-collar cybercrime" undoubtedly emerges as a concept worthy of further academic analysis and the hope that such theoretical evaluation can initiate and underwrite the fieldwork that the paradigm deserves.

References

Ames, J. (2019). Police cuts blamed as fraud cases fall. The Times, 9 December 2019, London.

Barlatier, J. (2020). Criminal Investigation and Criminal Intelligence: Example of Adaptation in the Prevention and Repression of Cybercrime. Risks, 8, ISS 99, 99.

Beck, U. (1992). Risk Society: Towards a New Modernity. London: Sage.

Berger, P. (1967). The Sacred Canopy: Elements of a Sociology of Religion. New York: Anchor Books.

Braithwaite, J. (1989). Crime, Shame and Reintegration. Cambridge: Cambridge University Press.

Brenner, S. W. and Koops, B. J. (2004). Approaches to Cybercrime Jurisdiction. Journal of High Technology Law, 4(1), 1-46.

Brown, R., Cannings, A., Sherriff, J. (2004). Intelligence-led vehicle crime reduction: an evaluation of Operation Gallant. Home Office Report 47/04, [Online] Available at:
https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.617.9003&rep=rep1&type=pdf (September 7, 2020).

Callanan, C., Jones, N. (2009). The Project on Cybercrime, UCD Centre for Cybersecurity and Cybercrime Investigation. Dublin: UCD.

Castells, M. (1996). The Information Age: Economy, Society and Culture. Oxford: Blackwell.

Castells, M. (2002). The Internet Galaxy: Reflections on the Internet, Business and Society. Oxford: Oxford University Press.

Clinard, M. (1983). Corporate Ethics and Management. London& New York: Sage

Clinard, M. and Quinney, R. (1973). Criminal Behaviour Systems: A Typology. University of Michigan: Holt, Rinehart & Winston.

Convention on Cybercrime, ETS No. 185, Budapest 23/11/2001, EU.

Dhillon, G. (2001). Computer crimes: Theorizing about the enemy within. Computers and Security, 20(8):715-723.

Friedrichs, D. O. (2002). Occupational crime, occupational deviance, and workplace crime: Sorting out the difference. Criminal Justice, 2(3), 243–256.

Friedrichs, D. O. (2009) Trusted Criminals, 4th Edition. Belmont, CA: Cenage Learning.

Fukuyama, F. (1996). Trust: The Social Virtues and The Creation of Prosperity. New York: Free Press.

Garland, D. (1996). The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society. British Journal of Criminology, 36(4), 445-471.

Gioia, D. A. (1992). Pinto Fires and Personal Ethics: A Script Analysis of Missed Opportunities. Journal of Business Ethics. 11, 379-389.

Gottschalk, P. and Gunnesdal, L. (2019). White-Collar Crime in the Shadow Economy: Lack of Detection, Investigation and Conviction Compared to Social Security Fraud. London: Palgrave Pivot.

Graves, J. T., Acquisti, A., Anderson, R. (2019). Perception versus Punishment in Cybercrime. The Journal of Criminal Law and Criminology. 109(2), 313-364.

Hagen, J.M., Sivertsen, T.K. and Rong, C. (2008). Protection against unauthorized access and computer crime in Norwegian enterprises. Journal of Computer Security, 16, 341-366.

Hall, S., Critcher, C., Jefferson, T., Clarke, J., Roberts, B. (1978) Policing the Crisis: Mugging the State and Law and Order, London: Macmillan.

Hamin, Z. (2000). Insider Cyber-threats: Problems and Perspectives. International Review of Law, Computers and Technology, 14(1), 105-113.

Harvey, J. and Lau, S.F. (2009). Crime-money, reputation and reporting. Crime, Law and Social Change, 52, 57-72.

Healy, P. and Serafeim, G. (2019). How to Scandal-Proof your company. Harvard Business Review, July August 2019. [Online] Available: https://hbr.org/2019/07/white-collar-crime(September 3, 2020).

Henning, P. J. (2020). What to Expect From White-Collar Prosecutions in 2020. The New York Times, January 14 2020, New York.

Hinduja, S. (2007). Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future. International Journal of Cyber Criminology, 1(1), 1-26.

Hobbs, S. and Hamerton, C. (2014). The Making of Criminal Justice Policy. Oxford: Routledge.

Holt, T. J. and Bossler, A.M. (2016). Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses. Oxford: Routledge.

Holt, T. J., Bossler, A. M., Seigfried-Spellar, K. C. (2017). Cybercrime and Digital Forensics: An Introduction. (2nd Edition). London: Routledge.

Hutchings, A. & Collier, B. (2019). Inside out: Characterising cybercrimes committed inside and outside the workplace. IEEE European Symposium on Security and Privacy Workshops, 17-19 June 2019, Stockholm: IEEE.

Irwin, N. (2020). It's the end of the world economy as we know it. The New York Times, 16 April 2020, New York.

Isenring, G. L., Mugellini, G., Killias, M. (2016). The willingness to report employee offences to the police in the business sector. European Journal of Criminology. 13(3), 372-392.

Jaishankar, K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal. International Journal of Cyber Criminology, 1(1), 1-6.

Jewkes, Y. (2003) Public Policing and Internet Crime. Jewkes, Y. and Yar, M. The Handbook of Internet Crime. Cullompton: Willan.

Johannes-Rose, K. (2020). De-risking or recontracting – the risk dilemma of EU money laundering regulation. The Journal of Risk Finance, 21(4), 445-458.

Kao, D.Y. and Wang, S.J. (2009). The IP address and time in cyber-crime investigation. Policing: An International Journal of Police Strategies & Management, 32 (2), 194-208.

Katz, D. A. and McIntosh, L. A. (2020) Politics and Purpose in Corporate America. Harvard Law School Forum on Corporate Governance, October 30, 2020. [Online] Available: https://corpgov.law.harvard.edu/ (October 31, 2020).

Koziarski, J. and Lee, J. R. (2020) Connecting evidence-based policing and cybercrime. Policing: An International Journal, 43(1), 198-211.

Kshetri, N. (2013). Cybercrimes in the Former Soviet Union and Central and Eastern Europe: Current status and key drivers. Crime, Law and Social Change, 60, 39-65.

Levi, M. (2007). Policing Financial Crimes. Pontell, H.N. and Geis, G. (eds.), International Handbook of White-Collar and Corporate Crime. New York: Springer.

Levi, M. (2008). White-collar, organised and cyber crimes in the media: some contrasts and similarities. Crime, Law and Social Change. 49, 365-377.

Mann, N., Devendran, P., Lundrigan, S. (2020) Policing in a Time of Austerity: Understanding the Public Protection Paradox through Qualitative Interviews with Police Monitoring Officers. Policing: A Journal of Policy & Practice. 14(3), 630-642.

Martin, J. (1973). Security, Accuracy, and Privacy in Computer Systems, New Jersey: Prentice-Hall.

McGee, J. and Byington, J. R. (2013). How to counter cybercrime intrusions. The Journal of Corporate Accounting and Finance, July/August, 45-49.

McGuire, M. R. (2011). Technology, Crime and Justice: The Question Concerning Technomia. Oxford: Routledge.

Molnar, J. (1987). Putting Computer Related Crime in Perspective. Journal of Policy Analysis and Management, Summer, 6(4), 714-716.

Neal, S. (2010). Cybercrime, transgression and virtual environments. Muncie, J., Talbot, D., Walters, R. (eds.). Crime: Local and Global. Cullompton: Willan.

Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., Whitty, M. (2014). Understanding Insider Threat: A Framework for Characterising Attacks. IEE Security and Privacy Workshops, IEE, 214-228.

Nykodym, N., Taylor, R., Vilela, J. (2005). Criminal profiling and insider cyber crime. Computer Law and Security Report, 21, 408-414.

Parker, D. B. (1976). Crime by Computer. New York: Charles Scribner.

Parker, D. B. (1979) Ethical Conflicts in Computer Science and Technology, Washington: AFIPS Press.

Parker, D. B. (1980). Computer-Related White-Collar Crime. Geis, G. and Stoutland, E. (eds.). White-Collar Crime – Theory and Research, Thousand Oaks: Sage.

Parker, D.B. (1983). Fighting Computer Crime, New York: Charles Scribner.

Payne, B. K. (2018). White-Collar Cybercrime: White-Collar Crime, or Both? Criminology, Criminal Justice, Law & Society, 19(3), 16-32.

Peretz Glazer, M. (1996). Ten Whistleblowers: What They Did and How They Fared. Ermann, D. M., and Lundman, R. J. (eds.). Corporate and Governmental Deviance: Problems of Organizational Behavior in Contemporary Society, 2nd Edition. Oxford: Oxford University Press.

Picard, M. (2009). Financial services in trouble: the electronic dimension. Journal of Financial Crime, 16 (2), 180-192.

Pickett, K.H.S. and Pickett, J.M. (2002). Financial Crime Investigation and Control. New York: John Wiley.

PwC. (2020) PwC'S Global Economic Crime and Fraud Survey 2020. [Online] Available: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html (October 30, 2020).

Ratcliffe, J. H. (2008). Intelligence-Led Policing. Cullompton: Willan.

Ratten, V. (2019). The effect of cybercrime on open innovation policies in technology firms. Information Technology & People, 32(5), 1301-1317.

Ring, S. (2016) U.K. White-Collar Prosecutions Rise as Cybercrime Threat Grows. Bloomberg.com, 23 May. [Online] Available: https://www.bloomberg.com/news/articles/2016-05-22/u-k-white-collar-prosecutions-rise-as-cybercrime-threat-grows (September 20, 2020)

Roach-Anleu, S. (2000). Law and Social Change. London: Sage.

Robertson, I. (1980). Social Problems. New York: Random House.

Seifert, R. and Mather, K. (2013) Neo-Liberalism at Work: A Case Study of the Reform of the Emergency Services in the UK. Review of Radical Political Economics, 45(4), 456-462.

Slingo, J. (2019). White collar crime prosecutions reach five-year low – despite rise in fraud reports. Law Society Gazette, 9 December 2019, London.

Sutherland, E. (1949) [1967] White-Collar Crime. New York: Holt, Rinehart and Winston.

Tackett, J. A. (2008). Covert investigations in the workplace. Journal of Corporate Accounting & Finance, 19(4), 7-11.

Taken-Smith, K., Jones, A., Johnson, L., Murphy-Smith, L. (2019). Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society, 17(1), 42-60.

Thomas, D. and Loader, B. (2000) (eds.). Cybercrime: Law enforcement, security and surveillance in the information age. London: Routledge.

Wall, D. (2007). Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press.

Willis, R. (1986). White-Collar Crime: The Threat from Within. Management Review, 75 (January), 22–32.

Wolf, M. (2020). The world economy is now collapsing. The Financial Times, 14 April 2020, London.

Yar, M. and Steinmetz, K. F. (2019). Cybercrime and Society. (3rdEdition). London: Sage.

Zheng, W., Yang, B., McLean, G.N. (2010). Linking organizational culture, structure, strategy, and organizational effectiveness: The Mediating role of knowledge management. Journal of Business Research, 63, 763-771.

.