Sheffield Hallam University

Financial crime in the twenty-first century: the rise of the virtual collar rriminal

REID, Alan <http://orcid.org/0000-0003-2019-5629>

Available from Sheffield Hallam University Research Archive (SHURA) at:

https://shura.shu.ac.uk/21674/

This document is the Accepted Version [AM]

Citation:

REID, Alan (2018). Financial crime in the twenty-first century: the rise of the virtual collar rriminal. In: RYDER, Nic, (ed.) White Collar Crime and Risk: Financial Crime, Corruption and the Financial Crisis. Palgrave Studies in Risk, Crime and Society . London, Palgrave Macmillan, 231-251. [Book Section]

Copyright and re-use policy

See http://shura.shu.ac.uk/information.html

Sheffield Hallam University Research Archive
http://shura.shu.ac.uk

Financial crime in the 21st Century: The rise of the Virtual Collar Criminal

Alan S Reid, Senior Lecturer in Law, Sheffield Hallam University

Abstract

This chapter introduces the phenomenon of virtual collar crime, that is quintessentially white collar crimes that are perpetrated entirely in cyberspace. Trust, trust dependency, high skill base criminals and opportunity zones were, and are, the hallmarks of white collar crime. The emerging paradigm of virtual collar crimes negates the requirement that perpetrators be highly skilled. Computer sagacity is no longer the *sine qua non* for cybercriminals - the phenomenon of 'Crime as a Service' has outsourced the skill requirement to third party providers of the required technological knowhow. Alongside the cascading down of such technical knowledge, twenty-first century society has driven headlong down the information superhighway, with hardly any area of human activity left unexposed to the effects of the ether. This perfect storm of increased virtuality and democratisation of online crime poses immense challenges to the entire twenty-first century society substratum, risking the future ability and desire of humans to interact with each other, have mutual trust and respect for one another and to have faith in established governmental institutions, commercial corporations and law enforcement. Legal systems must ensure that lives lived virtually are only exposed to an acceptable level of risk.

In the 21st Century, individuals, corporations and governments are becoming increasingly exposed to the risk of becoming victims of financial crime. The rise in white collar crime can be largely attributed to modern society's increasing reliance on electronic communications systems to control, monitor and deliver fundamental services. Schools, hospitals, companies, governments and households all rely on electronic communication networks to function properly. The exponential rise in ownership of powerful smartphones, tablets, portable gaming consoles, wearable computers and Smart TVs, allied with the growing availability of Wi-Fi hotspots and the phenomenon of the Internet of Things, have coalesced to revolutionise mobile computing and internet access. People are accustomed to working, playing, relaxing and socialising remotely and as such are constantly exposed to the danger of financial cybercrime.

Beyond the present, the future offers infinitely more opportunities for financial crime, as people's lives will be lived increasingly in the ether, through ubiquitous computing. The general phenomenon of cybercrime, although a relatively recent occurrence, is undergoing a paradigm shift in its modalities. Cybercrime is rapidly evolving to encompass increasing virtuality. Virtual money and financial systems, virtual representatives such as avatars, virtual memory and virtual imagery are just some examples of the increasing dimensions of electronic communications. Virtual money can be stolen or used to launder real-world

money, avatars can be attacked, destroyed or controlled by others and virtual intellectual property can be misappropriated. Further, virtual imagery that is illegal or offensive may be used and distributed for the purposes of blackmail and extortion. Virtual memory and resources hosted in the cloud can be stolen, modified or erased. Such virtual operations are often conducted anonymously or at least semi-anonymously and thus embolden the perpetrators of these white collar crimes that they can remain hidden in cyberspace, thus fuelling the preponderance of this type of crime. Thus, virtuality is promoting the rise of a new phenomenon, coined by the author as virtual collar crime.

This chapter outlines the rise of opportunities for virtual crime directed at individuals, corporations and governments and discusses what can be done to counter virtual financial cybercrime.

Introduction - white collar crime

The notion of white collar crime is well established and well documented. However, its definitional scope is incredibly fluid, porous, changeable and contestable. Historically, its classic exposition was espoused by the American criminologist Edwin Sutherland, in his famous book from 1949.[1]

For Sutherland, the defining features of white collar crime were the nature of the perpetrator and of the crime. It was a;

> 'crime committed by a person of respectability and high social status in the course of his occupation.'

The perpetrators invariably relied on their high occupational status, exemplified by the wearing of a white collar[2] and business suit, to inveigle their victims into suffering financial losses. The crime required a high level of trust dependency on the part of the victim towards the perpetrator and directly resulted in a loss of money or money's worth. The trust would be 'earned' by the perpetrator on account of their occupation, high position in society or high level of experience and skills and thus extended to business people, politicians and celebrities and not just middle and higher management employees of an organisation. This position of high status, high skill or high reputation enabled the perpetrator to engage in sophisticated abuses of that trust and position, without resorting to violence or threats of violence.[3] In terms of victims, the notion of white collar crime encompassed both individual victims who were overcome by the skills, position and reputation of the supposed trustworthy white collar operative and multifarious collective, innominate and diffuse victims such as legal corporations, local and national government, taxpayers and even abstract incorporeal notions such as the environment.

---

[1] *White Collar Crime*, E. Sutherland, 1949, New York: The Dryden Press.
[2] Hence the *modus operandi* and nomenclature of the crime.
[3] See, for example, A. Wright, *Organised Crime*, 2005, Willan Publishing, at p. 63.

Traditional white collar crime encompassed financial crimes such as bribery, embezzlement, money laundering, unfair competition, obstruction of justice and perjury, tax evasion and regulatory violations in fields like health and safety law, environmental law and food safety law.

Sutherland's definition came under increasing attack as being too simplistic, over-broad and undefined.[4] Nevertheless, the phenomenal rise in internet use globally has breathed new life into the general phenomenon of white collar crime.

The growth in general and specific cybercrimes, intellectual property infractions and novel crimes like health care fraud have required a new definitional approach to white collar crime. Further, the author posits that the growth of the internet has even created the possibility of a new definitional paradigm, that of virtual collar crime.

The lure of the Internet

Criminologists have argued that criminal offenders typically base their decision to engage in criminal activity on five variables: The effort that needs to be expended in committing the crime; the risk of detection; the rewards of the crime; the conditions that provoke criminal action and the ease of justifying or rationalising their behaviour.[5]

Thus cyberspace is a particularly attractive criminal space. For virtual collar criminals, cyberspace is an important enabler which reduces these barriers and helps to promote criminal behaviours and activities. The effort to be expended in committing crimes on the internet is low. Perpetrators no longer need specialised computing skills to perform cybercrimes, the crime can be conducted from the comfort of your own home, workplace or office anonymously and the crime can be conducted at any hour of any day, any day of the year. The rise of Virtual Private Networks (VPNs), TOR[6] browsers and end-to-end encryption mean that the risks of being identified during and after the cybercrime have been lowered. The rewards in cybercrime are potentially substantial, although the increasing incidence of cybercrime has had a deflationary effect on the price achievable for stolen identities and

[4] See, for example, the various critiques discussed by Hazell Croall - *Understanding white collar crime*, Croall, 2001, OUP, at pp. 6-7 and the discussion in Chapter 4, Computer Crime and White Collar Crime, Grabosky and Walkley, in *International Handbook of white-collar and corporate crime*, Pontell and Geis (eds.) Springer, 2007.

[5] See, for example, *Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention*, Cornish and Clarke, Crime Prevention Studies, 16 (2003), 41, *Understanding white collar crime*, Croall, OUP, 2001, and *The Oxford Handbook of White-Collar Crime*, van Slyke, Benson and Cullen (eds.), OUP 2016, particularly chapter 19 by Tamara Madensen, entitled *Opportunities for White Collar Crime*.

[6] Otherwise known as The Onion Router. TOR browsers allow internet users to surf the internet with a significantly enhanced level of privacy, akin to almost complete anonymity. The browser software, through a system of relays and encryption, routes connection information in a more private way such that it is incredibly time-intensive and difficult to trace individual users. The browser software is available at; https://www.torproject.org/download/download-easy.html.en.

other easily traded digital information. The atomised nature of online communications and crime allow for individuals to be actively encouraged to commit crime and thereafter to easily rationalise it as a victimless, small-scale crime.

Academics have identified four locations around which criminal activities coalesce. According to Felson, Hammer, Madensen and Eck[7], criminals obviously require a crime site itself, in order to perform the crime. This is the first place for crime - the crime site (*locus delicti*). Frequently, criminals will require the assistance of fellow conspirators in order to commit the crime and thus require a space to both interact with fellow criminals (Zone 2, identified as the convergence space setting) and a site to hide in and prepare for future criminal enterprise (Zone 3, the comfort space). The fourth zone is the corrupt spot, namely the place where further crime is encouraged from elsewhere.

In the real world, the *locus delicti* would be the home, the office, the workplace, the bank. Zones 2 and 3 would be the pub, the home, the gym or the car. Zone 4 would be places like recycling centres that incentivise the theft of valuable scrap materials.

The nexus of virtual collar crime is cyberspace itself and as such lends itself to a wide range of activities. Indeed, virtual collar crime is so appealing because all 4 zones of opportunity can be situated in cyberspace. The *locus delicti* (Zone 1) of the crime is the internet: for example stolen e-money, online services not paid for or theft of intellectual property. Zones 2 and 3 are similarly positioned in the ether: the e-games hub, social media sub-groups, special interest sites and the Dark Web. Zone 4 Corrupt Spots may also occur online: members of social media sub-groups, special interest sites and populations of the darkest reaches of the web may facilitate, support, encourage and create a market for the acquisition of illicit goods and materials and commission of online crime.

The Power Balance and the Changing Conception of White Collar Crime

The concept of white collar crime is predicated upon an imbalance in power between the perpetrator and the victim. In particular, the trust the victim places in the perpetrator rests on a certain level of ignorance and/or dependence on the part of the victim and a particular skill or attribute of the offender. The recent history of cybercrime has closely matched this white collar paradigm: the virtual victim has tended to be middle aged or older, be a newcomer to technology and thus under skilled and under prepared to defend themselves against the online threat; the virtual perpetrator has tended to be young, male and an enthusiastic adopter and user of new technologies and thus inordinately tech savvy and the online crime could only be committed by deploying specialist software or technological skills, for example through the creation and execution of malware, ransomware or computer viruses.

[7] As identified by Tamara Madensen, in chapter 19 '*Opportunities for White Collar Crime*' of *The Oxford Handbook of White-Collar Crime*, van Slyke, Benson and Cullen (eds.), OUP 2016, particularly.

In the second decade of the 21st Century, this paradigm no longer holds true: Victims of online crime are getting younger as technology becomes an established, all pervasive fact of life at an earlier and earlier age; victims in their teens or in their early twenties are digital natives and therefore tech savvy, not ill-prepared and unskilled in the digital environment; malware, ransomware and computer viruses are no longer bespoke, targeted complex computer programme codes beyond the reach of all but the best computer experts; generic programmes can be purchased off the shelf, via an online marketplace, or as an online crime application for smart phones and tablets; perpetrators no longer need a degree in computer science to create or execute online crime programmes and applications; in short the imbalance between the victim and the perpetrator has narrowed considerably.

This phenomenon is documented as 'Crime as a Service'.[8] Thus, the specialist skill required can now be outsourced and cascades downwards to the lower levels of criminal, who would have traditionally been thought of as blue collar criminals.

Blue collar crime is known as street level crime, frequently perpetrated by low-skilled males and encompasses physical attacks, threats of physical attacks and is highly visible and impactful. This type of criminal activity has a more direct bearing on people's quality of life, particularly physical attributes and as such society has tended to prioritise its resources on this type of overt criminal activity. White collar crime, by contrast, was relatively hidden, from the point of view of the victim, the harm caused and its societal impact and as such was given a much lower priority by law enforcement and the machinations of the state.

The future challenge for society is the increasing democratisation of white collar crime, such that these crimes can be committed by an increasing range of unskilled individuals and organised criminal gangs.[9]

Future virtual collar crime

In common with cybercrime generally the move to an online life has revolutionised the opportunity for criminal activity. Old crimes can be committed with increasing frequency and novel crimes are proliferating. Both the scale and scope of cybercrimes is increasing. Indeed the notion of 'crime as a service' means that the ability to successfully engage in online criminal activity is lucrative in itself, that is the virtual collar criminal can monetise his skills and knowledge in the virtual marketplace, selling his expertise to the online criminal masses. The greater propensity for humans living their lives online generates greater opportunities for virtual collar crime, as exemplified by a number of examples discussed below.

The Internet of Things

[8] See chapter 3 of the Europol Internet Organised Crime Threat Assessment 2014, available at; https://www.europol.europa.eu/iocta/2014/chap-3-1-view1.html.

[9] See for example the EUROPOL SOCTA report 2017, available at; https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

Internet connected laptop computers, tablets and smartphones are ubiquitous in the 21st Century, featuring in millions of homes, offices, factories and retailers across the globe. As such, the public are aware of the risks of going online and thereafter becoming a victim of cybercrime. However, the Internet of Things[10] looks set to magnify this risk by many factors in the coming years. As an example, within the European Union, research conducted by the European Commission estimates that there will be over 6 billion Internet of Things connections in Europe by 2020.[11]

The term 'Internet of Things' refers to the widespread deployment of Radio Frequency IDentifier 'RFID' enabled devices, products and furniture. RFID technology allows inanimate objects, previously seen as simply passive accoutrements of life, to actively collect and communicate information about their environment, position and status, remotely to servers and computers located anywhere in the world. Wide scale deployment of this technology posits an intelligent, ambient, fully controllable future. Thus, these passive objects are transformed into smart, active, technological computer devices and in so doing, liberates the internet, freeing it from its computer-based shackles. In so doing, the car, the fridge, the lightbulb, the oven, the toilet seat, the shower, the carpet, the cupboard, the desk, the door, the clothes on your back, the pacemaker and cybernetic enhancement[12] devices become receptors and repositories of valuable information.

This integrated seamless automated nirvana belies a serious criminal undercurrent, with this valuable information ready to be intercepted, modified, stolen or withheld by the virtual collar criminal. The risks associated with this technology are well documented.

At present, the increasing use of internet enabled apps to control vehicles or indeed to order taxis[13] mean that personal transportation is already vulnerable to criminal attack. The electronic systems that control battery and engine power, heating and air-conditioning and the alarm and the door openings could be controlled remotely and therefore be controlled by someone other than the driver or owner. Drivers or owners of electric cars could amend the power supply software so that they are charged less for their energy when plugged into the grid. Power to the engine and the controls could be switched off, making the car inherently dangerous, with the speed being increased to dangerous levels. Records of vehicle journeys could be made readily available online, much to the chagrin of the adulterer, the drug seeker or skiver.

---

[10] See for example, *RFID Tags and the EU: Really Free Internal Distribution?* Alan S. Reid *(2005) JITLP 4, 1-30,* at page 5.

[11] See *European Commission Report: Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination*, 2014, ISBN 978-92-79-47760-7, available at: https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination, at page 10.

[12] The term cybernetic enhancement refers to medical implants and devices that are inserted or attached to the human body, either to replace missing parts of the body or to enhance the functionality of existing body parts. See for example the discussion of this topic in; *The Future of Human Augmentation and Performance Enhancement*, Tracinski, 4th April 2017, Real Clear Science, http://www.realclearscience.com/articles/2017/04/04/the_future_of_human_augmentation_and_performance_enhancement.html.

[13] Via companies such as Uber, available at www.uber.com.

In the future, autonomous vehicles[14] will negate the need for humans to be in control of a vehicle at all, with every aspect of the car being controlled via artificial intelligence software. The car will select the most appropriate route and navigate through streets and motorways independently, avoiding other road users using anti-collision software.

Such ability to access critical information about the vehicle and to assume control of critical decision making software leaves the vehicle owner, the driver and passengers and the car manufacturer vulnerable to financial crime such as theft, blackmail, extortion and spurious personal injury claims.[15]

In the medical field, pacemakers, defibrillators or ventricular assist devices can be interrogated remotely by medical devices or can transmit their data via Wi-Fi, notifying the physician that it or the heart are not working properly. In the future, cybernetic enhancements such as bionic limbs, exoskeletons[16] and even brain augmentation implants will enable people to run and walk faster, lift and carry very heavy objects and receive and process information in the brain faster than at presently possible. In the field of entertainment, virtual reality games will increasingly rely on EEG[17] headsets to allow players to control the movement of avatars and control vehicles.[18]

The risk of a Wi-Fi enabled cyber-attack against a pacemaker, defibrillator or ventricular assist device, making the heartbeat or blood flow dangerously irregular, is not just a fantastical storyline for television drama, it is a realistic threat vector for opportunistic virtual collar criminals.[19] In a similar vein, in the future bionic limbs and exoskeletons could be susceptible to hacking attacks, rendering them inoperable or working at levels dangerous to human health. The deployment of brain augmentation implants may leave individuals vulnerable to the threat of psychological trauma. As the technology to read brainwaves through EEG headsets advances, hackers, using specialist algorithms, may even be able to

---

[14] That is driverless cars, controlled by artificial intelligence software. See, *Street Wars 2035: can cyclists and driverless cars ever co-exist? Laura Laker, 14th June 2017*, https://www.theguardian.com/cities/2017/jun/14/street-wars-2035-cyclists-driverless-cars-autonomous-vehicles.

[15] See for example: *Nissan Leaf electric cars hack vulnerability disclosed*, Leo Kelion, BBC News, 24th February 2016, http://www.bbc.co.uk/news/technology-35642749 ; *Mitsubishi Outlander hybrid car alarm 'hacked'*, BBC News, 6th June 2016, http://www.bbc.co.uk/news/technology-36444586 and http://www.bbc.co.uk/news/technology-35841571 .

[16] Exoskeletons are external skeletons that are attached to human bodies. They allow disabled people to walk and pick up objects and for soldiers and other professionals to carry heavy loads over a distance. See for example, *Rise of the human exoskeletons*, Neil Bowdler, BBC News, 4th March 2014, http://www.bbc.co.uk/news/technology-26418358.

[17] The term electroencephalograph, or EEG, refers to a machine placed on the head which can record electrical activity in the brain.

[18] See for example the commercial website of Neurosky, available at; http://neurosky.com/2015/09/eeg-games-top-5-list-playing-with-your-brainwaves/.

[19] The ex-vice president of the United States, Dick Cheney, reportedly requested that his pacemaker have no Wi-Fi capability after watching an episode of the American TV show Homeland: *Dick Cheney feared assassination by shock to implanted heart defibrillator*, Richard Luscombe, Guardian News, 19th October 2013, https://www.theguardian.com/world/2013/oct/19/dick-cheney-heart-assassination-fear.

accurately guess the passwords used by e-gamers to access the site, leaving them vulnerable to online theft and blackmail.[20]

Everyday items are and will be transformed by increasing deployment of the Internet of Things. The smart lightbulb, the smart carpet and smart heating thermostat controls can inform building owners of the number of people left in the building and alter the heating, lighting and security requirements of the building according to the fluctuating levels of occupancy over the course of the day in real-time, thereby achieving efficiency gains by saving energy, resources and money. Increased reliance upon software means that the building itself becomes vulnerable to hacking and remote control[21] by unauthorised individuals and groups, who can gain easy access to the building to steal or cause damage to the building.

More specifically, the ramifications for the power station,[22] air traffic control,[23] nuclear submarine defence,[24] care homes, water treatment plant or hospital[25] are immense. Critical infrastructure can be held to ransom, services can be disabled and utility services can be contaminated.

Smart fridges can interrogate RFID-enabled food and drink receptacles inside, notifying the owner that the milk has gone off or that the stock of white wine is critically low. The smart fridge can place an online order for milk or wine to be delivered, interrogate the smart door lock, causing the door lock to the house to open, ready for the supermarket delivery driver to enter and restock, all under the watchful eye of CCTV. The internet retailer Amazon has even invented the Amazon Dash button, a Wi-Fi enabled button allowing the replenishment of toilet rolls, razor blades and beer, which, in the future, could be delivered by drone.[26] This level of consumer immediacy and simplicity is a boon for busy households but could also be a mechanism for fraud. Smart fridge owners may hack the system to gain more supplies than they are actually invoiced for and neighbours may intercept deliveries by drone.

The Sharing Economy

---

[20] See for example, *Study Finds Hackers could use brainwaves to steal passwords*, Tiffany Westry Womack, June 29, 2017, Phys.org, available at; https://phys.org/news/2017-06-hackers-brainwaves-passwords.html.

[21] *Tomorrow's Buildings: Help! My building has been hacked*, Jane Wakefield, BBC Technology reporter, 20th April 2016, http://www.bbc.co.uk/news/technology-35746649.

[22] See the discussion in; *Hackers behind Ukraine power cuts*, says US report, BBC News, 26th February 2016, http://www.bbc.co.uk/news/technology-35667989.

[23] Remote and Virtual Tower control allows air traffic to be controlled remotely rather than from the control tower at the end of a runway. National Air Traffic Services, Press Release, 19th May 2017, available at; http://www.nats.aero/news/london-city-airport-and-nats-to-introduce-the-uks-first-digital-air-traffic-control-tower/. However, it could be argued that such a system may be more susceptible to hacking than pre-existing computer navigation systems.

[24] See the report, *Hacking UK Trident: A Growing Threat*, Stanislav Abaimov and Paul Ingram, British American Security Information Council, 1st June 2017, available at; http://www.basicint.org/publications/stanislav-abaimov-paul-ingram-executive-director/2017/hacking-uk-trident-growing-threat.

[25] The UK's National Health System computer system was taken down by the WannaCry ransomware worm on the 12th of May 2017: *What is WannaCry ransomware and why is it attacking global computers?* Alex Hern and Samuel Gibbs, 12th May 2017, Guardian online, https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20.

[26] See the Amazon website: https://www.amazon.co.uk/Andrex-Dash-Button/dp/B01I29IZQ6.

The phenomenal rise in online commerce, particularly consumer to consumer transactions (C2C) has resulted in a significant rise in the risk of opportunistic online financial crime. The 21st Century has also seen the rise of what has been called the Sharing Economy[27]. The Sharing Economy[28] refers to People to People (P2P) networks whereby people connect over the internet to share human, physical and intellectual resources, typically on a reciprocal, non-monetary basis.

Sites like AirBnB[29], Uber[30], eBay[31], Amazon Marketplace[32] and Craigslist[33], have revolutionised commerce conducted via cyberspace. They have disrupted traditional commerce models such as Business to Business (B2B) and Business to Consumer (B2C). They are based on the principle of connecting buyers and sellers on a many to many basis. As such, they reduce the professional and commercial links of traditional B2C business and replace this with a horizontal transactional relationship between private individuals. This change in relationship promotes riskier behaviour and a greater exposure to fraudulent activity. The main laws on consumer protection do not apply to C2C transactions.

Consumer to consumer fraud is multifarious. Examples include online sellers sending their products to the buyer, only for the buyer to claim that no such product arrived.[34] It appears that unscrupulous sellers are able to substitute the real goods with other inferior or cheaper objects and then claim that the goods never arrived or were damaged in transit. Under the contractual terms of eBay, the buyer is arguably more strongly protected than the seller under the terms of the Money Back Guarantee[35] and therefore unscrupulous buyers can invoke the redress system before the seller has had an opportunity to tell their side of the story and therefore receive reimbursement from eBay, which then seeks recompense from the seller.[36]

Cryptocurrencies

---

[27] See the definition adopted by The People who Share website: http://www.thepeoplewhoshare.com/blog/what-is-the-sharing-economy/.

[28] For an overview of some of the contractual risks associated with the Sharing Economy, see *Digital Revolution: Challenges for Contract Law in Practice*, Schulze and Staudenmeyer (eds.), Nomos/Hart Publishing 2016.

[29] The website for Airbnb is https://www.airbnb.co.uk/.

[30] The wesbite for Uber is https://www.uber.com/.

[31] The wesbite for eBay is http://www.ebay.co.uk/.

[32] Information on Amazon.co.uk Marketplace is available at http://www.amazon.co.uk/gp/help/customer/display.html?nodeId=3149141.

[33] The wesbite for Craigslist is https://www.craigslist.org/about/sites.

[34] *It's seller beware as eBay's buyer guarantee is exploited by scammers*, Anna Tims, 25th April 2016, http://www.theguardian.com/money/2016/apr/25/ebay-seller-beware-buyer-guarantee-exploited-scammers?CMP=share_btn_link.

[35] The Terms and Conditions of the eBay Money Back Guarantee in the United Kingdom are available at: http://pages.ebay.co.uk/help/policies/money-back-guarantee.html#receive.

[36] See the discussion in the Guardian Online article: *It's seller beware as eBay's buyer guarantee is exploited by scammers*, Anna Tims, 25th April 2016, http://www.theguardian.com/money/2016/apr/25/ebay-seller-beware-buyer-guarantee-exploited-scammers?CMP=share_btn_link.

The exponential rise in interconnected computer networks and the concomitant rise in online transactions globally, created a desire for a truly online method of payment, freed from the shackles of the traditional banking system. Thus, the past few years has seen the rise of alternative payment systems like PayPal but also the creation of virtual currencies, based on peer-to-peer technology[37]. The most famous crypto-currency is that of Bitcoin. These decentralised systems of exchange offer tremendous advantages over traditional transfers of moneys' worth that require the involvement of financial services providers acting as third party intermediaries, which charge a fee and inevitably cause a delay in transferring the funds, adding to the overall cost of the transaction. Involving a third party in the transaction also increases the risk of the underlying transaction not being fulfilled, due to delay, misplacement of the funds or the financial service provider refusing to authorise the transfer[38].

Nevertheless, reliance on crypto-currencies is not without significant risk of becoming a victim of virtual collar crime. In the case of new, emerging currencies, there is always a nascent phase in their development in which the currency is pre-mined, in order to generate enough critical mass of the currency to trade in.[39] Once the currency is established, users of crypto-currencies face the risks of extreme volatility in the real world value of currency, the lack of convertability into real world currencies, and the general cybercrime risks of malware, ransom requests and theft.

The Dark Web (and the Light Web)

The anonymous dark web has now entered the public consciousness and is utilised for both legal and illegal means. The privacy afforded by the use of technology such as TOR emboldens internet users, in a positive sense, to criticise their repressive government, expose illegal activity of their politicians, organise legitimate protests and demonstrations and to communicate with like-minded individuals, free of governmental surveillance.

This privacy is clearly also highly attractive for more negative applications over the internet. The Dark Web facilitates significant trade in controversial products and services such as legal and illegal drugs, child abuse imagery, weaponry[40], pirated intellectual property,

---

[37] For an overview of crypto-currencies, see *Chapter 9: Virtual currency in a virtual world: virtually unstoppable?* Alan S. Reid, in *Fighting Financial Crime in the Global Economic Crisis,* Ryder, Turksen, Hassler (eds.), Taylor and Francis, 2014.

[38] See *Chapter 9: Virtual currency in a virtual world: virtually unstoppable?* Alan S. Reid, in *Fighting Financial Crime in the Global Economic Crisis,* Ryder, Turksen, Hassler (eds.), Taylor and Francis, 2014, at p. 172.

[39] See *Chapter 9: Virtual currency in a virtual world: virtually unstoppable?* Alan S. Reid, in *Fighting Financial Crime in the Global Economic Crisis,* Ryder, Turksen, Hassler (eds.), Taylor and Francis, 2014, at p. 176.

[40] *Online retail boom helping criminals smuggle guns into UK, says police chief*, Vikram Dodd, 28th February 2016, Guardian Online, http://www.theguardian.com/uk-news/2016/feb/28/online-shopping-boom-criminals-smuggle-guns-uk-police-chief?CMP=share_btn_link.

endangered animals and their by-products[41] and looted art and artefacts, of dubious provenance[42].

However, even the World Wide Web itself is a vector in the sale of such prohibited goods and services. The sheer scale and scope of the membership of social media sites[43] means that like-minded individuals and organisations can easily find one another and arrange the exchange of contraband across borders, with the management of social media sites simply overwhelmed with the task of identifying, monitoring and enforcing criminal law violations taking place on their networks.

Online Dating, Companionship and Revenge Porn

In the cash rich, time poor 21st century, the quest for love and human companionship has gone virtual, with a tremendous uptake of social media sites and apps like Tinder[44], Ashley Madison[45] and Grindr[46] and online dating sites like match.com[47] and eharmony.com[48]. Naturally, the scope for falsity in virtual/remote relationships is immense, since in order to improve the prospects of successful dating and friendship, people will invariably want to paint themselves in the best light and may decide to cut corners by posting pictures of other people on their profile, embellishing their interests and achievements or creating absolute falsehoods.[49] There is also an enhanced risk of becoming the subject of blackmail, extortion, identity fraud and identity theft. Blackmail and extortion are a real risk where the individual is in a long-term relationship of marriage or civil partnership and actively seeking sexual partners outside of that long-term relationship or where the individual is seeking a sexual partner online, that is different to their known sexual preference(s). Identity fraud and theft are a risk simply because the dating apps and sites, by definition must collect, retain and use sensitive personal data of its users in order to provide the dating service itself. The hacking of the Ashley Madison site, exemplifies the range and nature of this risk.

The atomised, distant nature of online interaction facilitates such behaviour. However, recent developments have augmented this activity. The process of relationship finding

---

[41] See *Wildlife Smugglers using Facebook to sell ivory and rhino horn*, Jeremy Hance, 14th November 2016, Guardian News, available at; https://www.theguardian.com/environment/2016/nov/14/wildlife-smugglers-using-facebook-sell-ivory-rhino-horn.

[42] See *How Western art collectors are helping to fund Isis*, Leila Amineddoleh, 26th February 2016, Guardian News, available at; https://www.theguardian.com/artanddesign/2016/feb/26/western-art-funding-terrorism-isis-middle-east.

[43] Indeed, it has been reported that Facebook may well amass 2 billion users by the end of 2017: *Facebook is closing in on 2 billion users*, Seth Fiegerman, 1st February 2017, CNN, available at; http://money.cnn.com/2017/02/01/technology/facebook-earnings/index.html.

[44] The website to download the app is available at; http://www.gotinder.com.

[45] The website is available at; http://www.ashleymadison.com.

[46] The website is available at; http://www.grindr.com.

[47] The website is available at; http://www.match.com.

[48] The wesbite is available at; http://www.eharmony.com.

[49] *Tinder nightmares: man scams two women out of $26,000*, Julia Carrie Wong, Guardian Newspaper, 17th February 2016, http://gu.com/p/4gz7n/sbl.

online can now be outsourced for a fee, with companies and individuals offering to organise and operate an individuals' online dating account.[50]

If finding a real-life partner is too complicated, or a person is under familial pressure to be in a long-term relationship, technology offers a solution in the shape of a virtual girlfriend or boyfriend. Apps like Virtual Girlfriend and KARI, allow people to interact with an artificial intelligence computer system. The virtual companion will respond to the user's communications and can even send messages to friends and family that convincingly appear to come from a real person.

Internet connectivity in the bedroom may result in a loss of libido and/or physical intimacy in a relationship, however adult toys that are Wi-Fi enabled can lead to more serious problems of a legal nature. Beyond the obvious privacy concerns[51] that may arise from usage data being stored in the cloud by the toy manufacturer, users may be susceptible to hackers resorting to blackmail or extortion.

The video capture technology in the palm of everyone's hand has led to the modern phenomenon of revenge porn. The ability to easily record high quality images and sounds in a compact smartphone or tablet means that amateur pornography has gone mainstream. Self-made pornography, consensual recording of intimate bodily areas or activities or surreptitious non-consensual filming of such activities all share one characteristic: the ability to be uploaded and shared online by the ex-lover, the stalker, the voyeur and the hacker. The phenomenon of revenge porn does not squarely fall within the broad definition of white collar crime. Nevertheless, the consequences of such actions do clearly fit the definitional matrix. An online industry has developed whereby, for a not inconsiderable fee, websites hosting this material will gladly take down the offending images.[52] Indeed, the commercialisation and professionalism of the websites exhibit the classic white collar paradigm.

Algorithms

This utopic (or dystopic) online environment relies heavily upon complex algorithms to work. At present, individuals are accustomed to automated decision making, particularly when they apply for a loan or a mortgage. Artificially intelligent entertainment services already allow people to talk to devices that can suggest recipes to cook, TV shows and films to watch, games to play and music to listen to. Social media sites use algorithms to direct content to users that is exciting, entertaining and enticing, according to their demographic.

---

[50] Virtual Dating Assistants and Invisible Girlfriends. *Invisible Girlfriends: a dubious service for dubious customers*, Eleanor Robertson, Guardian Newspaper, 29th August 2014, http://www.theguardian.com/commentisfree/2014/aug/29/invisible-girlfriend-a-dubious-service-for-dubious-customers

[51] See the article, *Sex Toy Maker Pays $3.75 Million to Settle 'Smart' Vibrator Lawsuit*, Jeff John Roberts, March 10, 2017, Fortune, available at; http://fortune.com/2017/03/10/sex-toy-maker-settlement-smart-vibrator-lawsuit/.

[52] *Revenge porn: the industry profiting from online abuse*, Dan Tynan, Guardian Online, 26th April 2016, https://www.theguardian.com/technology/2016/apr/26/revenge-porn-nude-photos-online-abuse?CMP=share_btn_link.

In the future, algorithms will control the driverless car and the conversation with a virtual assistant will be indistinguishable with interactions with humans.

Altering the algorithm offers significant scope for financial crime. The applicant could secure a better loan rate for themselves or hackers or financial service employees could force the applicant to accept an artificially worse loan rate, with the virtual criminal pocketing the monetary difference. Entertainment service and social media algorithms could be modified by individuals to direct and monetise traffic to content and websites controlled and operated by that individual or their associates.

Virtual Collar Crime solutions?

As this overview of the near future provides, increased online living is accompanied by an increased risk of being a victim of virtual crime. The UK's National Audit Office has recently grappled with this phenomenon and has highlighted significant deficiencies in the UK's preparedness[53].

The report found that in 2016, in England and Wales, there was estimated to have been 1.9m separate cyber-related fraud events, equating to 1 in 6 adults experiencing fraud, making online fraud the most commonly experienced crime[54]. However, recorded fraud incidents for the same period only totalled 623,000, indicating a massive problem with under-reporting[55]. Collectively, these individual cyber-frauds are calculated to cost individual victims a loss of £10 Bn and businesses £144 Bn[56]. Crime of this magnitude, scale and scope should be one of the highest priorities for law enforcement within the UK. However, according to the National Audit Office, only 1 in 150 police officers have, as their main function, the investigation of economic crime[57]. Further, more than a third of Police and Crime Commissioners in England and Wales omitted to mention online fraud at all in their annual plans for 2017[58].

Individuals and organisations, who wish to be proactive and minimise their exposure to online fraud are faced with a bewildering array of advice sites, creating the risk that the educational message is lost, contradictory or out of date[59].

The fragmented, disparate and individualised nature of virtual collar crime means that it is difficult to coordinate, plan and enforce the law in a coherent way. The victims, offenders, modalities, scale and effect of virtual collar crimes are extremely heterogeneous. Thus, a one-size fits all approach to tackling the phenomenon will not work. This diversity is also replicated in the approach taken to these crimes by the police in England and Wales,

---

[53] *Online Fraud*, National Audit Office, 30th June 2017, ISBN: 9781786041241.
[54] *Online Fraud*, National Audit Office, at p. 2 of the executive summary.
[55] *Online Fraud*, National Audit Office, at p. 2 of the executive summary.
[56] *Online Fraud*, National Audit Office, at pp. 2 and 3 of the executive summary.
[57] *Online Fraud*, National Audit Office, at p. 2 of the executive summary.
[58] *Online Fraud*, National Audit Office, at p. 2 of the executive summary.
[59] *Online Fraud*, National Audit Office, at p. 2 of the executive summary. The report found that there were at least 10 campaigns live in March 2017, dedicated to education and awareness raising as regards online fraud.

exacerbating the discrepancy in approach across the country, with pockets of best practice not being rolled out across the entire UK. The City of London police, with their geographical location in the heart of the UK's financial district, are in a privileged position to take the lead in the fight against online crime, alongside the National Fraud Intelligence Bureau and the National Crime Agency[60]. However, even with only three bodies involved, there is scope for gaps to appear, contradictory approaches, for best practice to remain localised and for duplication of effort. The international nature of many virtual collar crimes means that cooperation between law enforcement, prosecuting authorities and the judiciary needs to be maintained and enhanced with the UK's partners both within the EU and with the rest of the world. At the level of prosecutions and sentencing, there is also wide divergence in the rate of prosecutions and the sentences handed out across England and Wales[61]. In the past, these discrepancies could be dismissed as being the result of crime being a localised or regional phenomena that did not take place uniformly across the country and sentence diversity simply reflected the multifarious permutations of fraud. However, in the 21st Century, no village, hamlet, town or city is immune from the risk of virtual collar crime and the diversity of the typologies of virtual collar crime do not justify a corresponding diversity in sentencing. Stolen intimate photographs, the theft of a Bitcoin, inflated loan repayment schedules or a non-existent holiday apartment booked and paid for online all share the same basic white collar characteristics: A betrayal of trust and significant financial and non-financial damage to the victim and as such sentencing should reflect the level of individual and societal harm caused, societal opprobrium of the conduct and a proportionate deterrent effect.

Conclusion

A perfect storm of increased internet penetration and pervasiveness, reduced complexity in the creation and operation of internet apps and services, and the growing realisation of the profitability of the 'Crime as a Service' model and of assisting criminal activity online, has transformed the concept of white collar crime.

The history of white collar crime is replete with examples of technological developments being used to incorporate facets of what can now be termed virtuality: The telegraph, the phone, the cheque, the fax, the credit and debit card and the computer all provided increasing physical distance between the white collar criminal and the victim. However, 21st Century technology has been truly transformative. Digitisation means that virtually all physical and non-physical crimes classified as being of the white collar genus can be committed in cyberspace. The defining characteristic of white collar crime has been that it is committed by a person who is in possession of technical expertise or skills and is therefore in a position of trust. That trust forms the basis of an imbalanced power relationship which is then abused to commit financial crime. However, white collar crime has transcended these limitations. The expertise and skill of the white collar criminal is now easily obtainable and sophisticated computer programmes and algorithms offer the authenticity, professionalism and competence required to engender trust.

[60] *Online Fraud*, National Audit Office, at p. 8 of the executive summary.
[61] *Online Fraud*, National Audit Office, at p. 8 of the executive summary.

The growing usage of online horizontal commercial, business, social and professional platforms, the rise of the Internet of Things, the simplification and ease of access of internet apps creation and their deployment and the development of the 'Crime as a Service' model has created the phenomenon of Virtual Collar Crime.

The law needs to be more attuned to these dangers. Small scale, individual virtual crimes must be aggregated to highlight the collective, cumulative danger to society. As developed societies are driven towards ever more online dependency, these virtual risks will only increase exponentially. Legal developments also need to go hand in hand with an upscaling of digital skills for the general population so that individuals and organisations can better defend themselves and prevent them becoming victims. Otherwise, society faces an unprecedented reversal of technological advancement as we lose all semblance of trust in the internet: A Winter of Disconnect.