Pandemics and fraud – Learning from the coronavirus pandemic and its antecedents

Michael Levi

Introduction

Covid-19 is the first pandemic of the universal cyber age. This collection is about cyber crimes, and therefore all previous pandemics are arguably irrelevant except as potential exemplars of what little evidence there is of the impact of previous pandemics on fraud (Levi and Smith, 2021). Fraud has not hitherto been a feature of major books on pandemics in general or covid-19 in particular, though in addition to an array of 'deep state' conspiracy texts, there are books with enticing titles like *Unraveling the CoVid Con*, *Covid-19: Exposing The Lies*, *The Great Covid Deception*, *Captured by COVID: Deceit, Conspiracy & Death—A True Story, Autopsy of a Pandemic: The Lies, the Gamble, and the Covid-Zero Con*, and *Transcending the Covid-19 Deception* – none of them about fraud or scams as understood within the framework of this book. Reitano and Shaw (2021) wrote an eloquent popular text - *Criminal Contagion: How Mafias, Gangsters and Scammers Profit from a Pandemic*- about how organised criminals (but not otherwise licit corporations) were exploiting the pandemic, but that was about it. The term 'major book' or 'serious book' is a contested space, but none of those mainstream texts contain anything about fraud beyond the construct that governments falsely constructed the risks and harms of covid (see Dodsworth, 2021, for a more sophisticated analysis thereof).

Nevertheless, outside of books, a small cottage industry in tracking the impacts of covid-19 on crime generally and cyber-enabled fraud in particular has developed in journals and government publications. Risks and threats to current and future processes in the 'cyber' world are ubiquitous (as they are to other arenas of 'transnational' crime), but there are boundary issues about financial crime and technology going back to the invention of the telegraph, which transmitted money and information almost instantaneously, enabling fraudsters as well as non-fraudsters to send money internationally a great deal faster than by ship or overland. These should be borne in mind when considering the impact of 'cyber' on fraud.

Many readers coming of age this century may struggle to envisage a cyber-less world, and especially since the COVID-19 pandemic began, the commentariat has been obsessed with online fraud. Online fraud is often presented as a binary opposite to offline fraud but, as we shall see, the two often combine. Except where electronic communications and payments are not used at all, there is very little significant fraud that is not at least cyber-assisted in the late modern era, and routine administrative data

collection is unlikely to preserve accurately the distinction between cyber-dependent, cyber-enabled, cyber-assisted, and entirely offline fraud (Wall, 2007).

The law enforcement and media focus is often on 'organised crime groups' moving into fraud – principally the scams created from a distance electronically by youths in hoodies operating from their bedrooms or by West African or Eastern European diasporas (Levi, 2008; Lusthaus, 2018; Whitty, 2018; Lusthaus and Varese, 2021), plus ransomware and hacking from state-sponsored and state-tolerated groups in China, North Korea or Russia – all of them 'outsiders' to their victims. But we must also consider the impact of the pandemic on insider frauds, which involve executives or IT-savvy staff colluding with others or dominating companies they run.

In many other fraud cases, especially those committed by insiders, there is a long elapsed time between the commission of fraud and its detection by the victim or a public or private sector third party. Choice of offender or victim location is determined by other factors (such as the large number of relatively wealthy but still emotionally anxious retired people in Bellevue Hill Sydney or in the South East of England). In the larger cases, professional intermediaries and bank accounts are necessary components in presenting a plausible front and in obtaining and laundering the funds; in others, cash may be wired via Money Service Bureaus (like Western Union) or by 'underground banking' to foreign or sometimes domestic locations.

Measuring frauds and 'the fraud problem' – from offline to online?

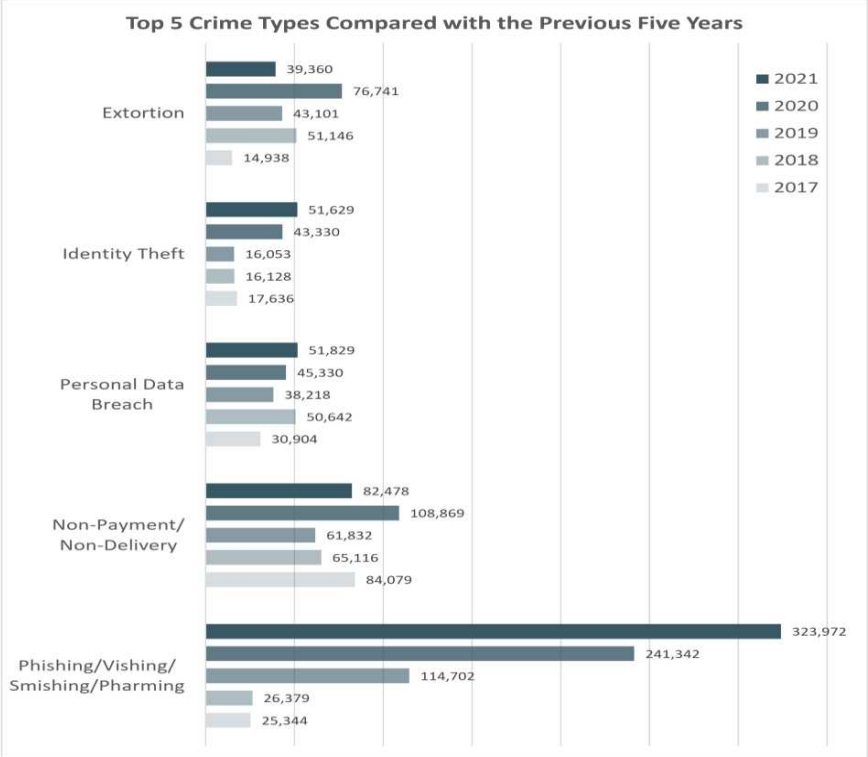
How do we know what impact the pandemic has had on fraud? Bentham proposed keeping crime statistics for better administration of changes in (im)moral behaviour, and by this criterion, fraud and cybercrime have not been important indicators to many nations. Furthermore, the framers of the crime victimisation surveys did not contemplate the inclusion of offline or online frauds, and fraud (or corruption and money laundering) recording has not received much input in revisions of crime statistics over decades. We might expect the revelations about the harmfulness and prevalence of frauds and cybercrimes to generate or give impetus to a certain 'moral panic' and make it hard for politicians and police chiefs to deny resources. But this is an open empirical question, and it also relates to the issue of whether increasing fear of crime is always a bad thing. Without fear, we may not take sufficient precautionary measures, and the suppliers of goods and services may not have sufficient pressure to take security seriously.

Digital fraud in North America

The annual reports from the FBI Internet Crime Complaint Center (IC3) are very detailed, with complaints rising from 49,711 complaints in 2001 to over 5 million reports in 2021 of thefts, scams, frauds, and other crimes with an online nexus. The

crimes reported to the IC3 also reflect scammers' willingness to exploit various tragedies and disasters, such as Hurricanes Rita and Katrina as well as after the Boston Marathon bombings. During the COVID-19 pandemic, scammers have been hawking fake cures and investments schemes, selling personal protective equipment at high profits without having it available, and looking to take advantage of a more concentrated online presence during a time of increased teleworking and distance learning (see Levi and Smith, 2021).[1]

The largest leap in each category was end 2019-end 2020. It is not clear what proportion of these scams led to actual financial losses, although they can lead to emotional or time/repair costs irrespective of whether frauds were attempted or were successful.



Digital frauds in Europe

The Eurobarometer delivers the only cross-national comparative data collection on victimisation of some types of fraud in the EU, showing clear variation in identity theft levels between countries. In 2019, before the pandemic began, half of all respondents knew of someone who had been a victim of one of the cybercrimes asked about, with

[1] www.fbi.gov/news/stories/ic3-20th-anniversary-050820.

the most mentioned being receiving fraudulent emails or phone calls asking for personal details (25 per cent) or discovering malicious software on their device (21 per cent) (Eurostat, 2019). However, only a minority of respondents have personally been a victim of any of the cybercrimes listed in the questionnaire, with the most common being receiving fraudulent emails or phone calls asking for their personal details (36 per cent) or discovering malicious software on their device (28 per cent). Victims of bank card or online banking fraud (84 per cent), online fraud or identity theft (both 74 per cent) are the most likely to say they took action as a result. In each of these cases respondents most often contacted the police or the website or vendor.

Data are best on volume fraud, especially payment card fraud, which worldwide rose from $17.5 to an estimated $20 billion in 2020–21.[2] Most European data are released much later than those in the UK (and were so before the UK left the EU) – for example, a review of EU payment card fraud data in 2019 was released in October 2021 (ECB, 2021). It showed that even in 2019 – pre-pandemic – 80 per cent of card fraud took place via online and mobile payments, while 15 per cent took place in shops and 5 per cent at ATMs; and cross-border transactions accounted for 65 per cent of the total value of card fraud.

The UK

UK data on payment card fraud have always this century been much better and more detailed, and more up to date (UK Finance, 2021): in recent years, the largest fraud losses have been unauthorised frauds, mainly committed using payment cards. There was some question whether offline traditional crime was merely displaced by less well measured online crimes. The then UK Prime Minister intriguingly omitted the considerable rise in fraud when claiming in 2022 that ‘crime’ had fallen under his administration.[3] He was later backed up by his Secretary of State of Business, who asserted on BBC television that ‘The point the prime minister was making is that the crime that people experience in their day to day lives, in terms of fraud, in terms of burglary – well not fraud, but in terms of burglary, in terms of physical injury has gone

[2] www.statista.com/statistics/1273177/ecommerce-payment-fraud-losses-globally/

[3] https://hansard.parliament.uk/commons/2022-01-31/debates/6B412B49-AB7D-4FE3-9F82-B9EAE93FB6AC/SueGrayReport, col.24; https://www.dailymail.co.uk/news/article-10473803/Watchdog-blasts-Johnson-Patel-claiming-crime-fallen-14-fact-RISEN.html).

down. That's absolutely right.'[4] This downplaying of fraud victims was not well received by the media, politicians and public.

Differently expressed, the risks of crime in the UK vary considerably by crime type, and both fraud and computer misuse offences outstrip all other property crime risks directly affected individuals. This was so before the pandemic, but the trend increased during it, as more people of all ages migrated their legal (and a little of their illegal) consumption online and spent far more time on it.

The Netherlands

A one-off Dutch study in 2011 (Domenic et al., 2013) showed that of those using auction sites, 3.4 per cent were victimised by some version of auction fraud (like eBay). Less than 1 per cent of the respondents had been victimised by identity fraud on the internet, but among that group, certain internet practices, like participating in contact or dating sites, seem to contribute to the chances of being victimised through internet identity fraud. A Central Bureau of Statistics Netherlands general population study of identity fraud, consumer sales fraud and hacking by Kloosterman (2015) showed that hacking was the most common form of cybercrime in 2014, affecting more than 5 per cent of the population, followed by acquisitions and sales fraud (3.5 per cent) and identity theft (less than 1 per cent). The recent Dutch Safety Monitor (2022) shows that by 2021, 10 per cent of the Dutch population had become a victim of online scams and fraud, 7 per cent of hacking, 2 per cent of online threats and intimidation, and 1 per cent of other online crimes. In 2021, more than two in three (68 per cent) of all Dutch people aged 15 and older say that they have received a phone call, email or other message at least once in the past 12 months that (probably) was from a scammer. Some 2 per cent indicate that they have fallen for this at some point. Almost half of these (0.8 per cent) eventually lost money.

Sweden

The Swedish Crime Survey 2014 showed that the percentage of people exposed to fraud gradually increased from 2.5 per cent in 2006 to 3.5 per cent in 2013 before falling to 3.1 per cent in 2014, and 44 per cent of these involved the Internet. The only acquisitive crime more common than fraud in Sweden is bicycle theft. A total of 84 per cent of victims stated that this was a single event, but this still leaves 1 in 6 fraud victims suffering multiple victimisation (some of them being presumably multiple card fraud

[4] https://www.mirror.co.uk/news/politics/tory-defends-boris-johnsons-lies-26153680

victims). Median losses were under 10,000 Kroner (£817/$1,171). In terms of recorded fraud, compared with 2013, Computer Fraud increased by 25 per cent to 42,900 reported crimes. See further: www.bra.se/bra/brott-och-statistik/bedragerier-och-ekobrott.html.

Of the Swedish population (aged 16–84), 5.5 per cent state that they were victims of sales fraud in 2020. This was a rise from 2019 (5.1 per cent), and an increasing trend can be seen since 2016 when the percentage of self-reported victimisation was 4.5 per cent. Men (6.4 per cent) state that they were victims of sales fraud in 2020 more often than women (4.6 per cent). Sales fraud was most common in the 35–44 age bracket among men (9.0 per cent) and in the 45–54 age bracket among women (6.1 per cent). Card fraud victimisation affected 4.1 per cent of the population in 2020, compared with 5.3 per cent in 2019, perhaps because people went less to risky places during the pandemic or perhaps because of greater prevention efforts. Men (4.6 per cent) were victims of card/credit fraud more often than women (3.6 per cent). The most common age bracket for card/credit fraud was 45–54, where 6.6 per cent of the men and 4.9 per cent of the women state they had been victims of card/credit fraud.

Fraud in Asia-Pacific

For illustrative purposes, I select two jurisdictions in Asia Pacific, although very good detailed police recorded cybercrime and arrests data are available for South Korea (www.police.go.kr/eng/statistics/statisticsSm/statistics04.jsp), which show variations in rising cybercrimes and arrests 2014–2020: cyber fraud has more than doubled in that time.

Hong Kong

The Hong Kong police was an early convert to the importance of cybercrime, and in 2014, it was made a priority for the police Cyber Security and Technology Crime Bureau. The following tables show the rise in both the costs and numbers of reported crime. The annual reports helpfully utilise a category of technology crimes, which have been rising substantially as other recorded crimes have been falling or static. Note the boom in the number of cases (but not financial losses) 2019–20. It is not known how accurately the financial losses are calculated.

Year	Financial loss (HK$ million)		Number of cases
2020	2,964		12,916
2019	2,907		8,322
2018	2,771		7,838
2017	1,393		5,567
2016	2,300		5,939
2015	1,828		6,862
2014	1200		6,678
2013	916		5,133
2012	340		3,015
2011	148		2206
2010	60		1643
2009	45		1506

Table 26.2 Number of recorded cases and the financial losses due to reported computer crime in Hong Kong (Hong Kong Police Force: available at:

Digital crimes in Australia

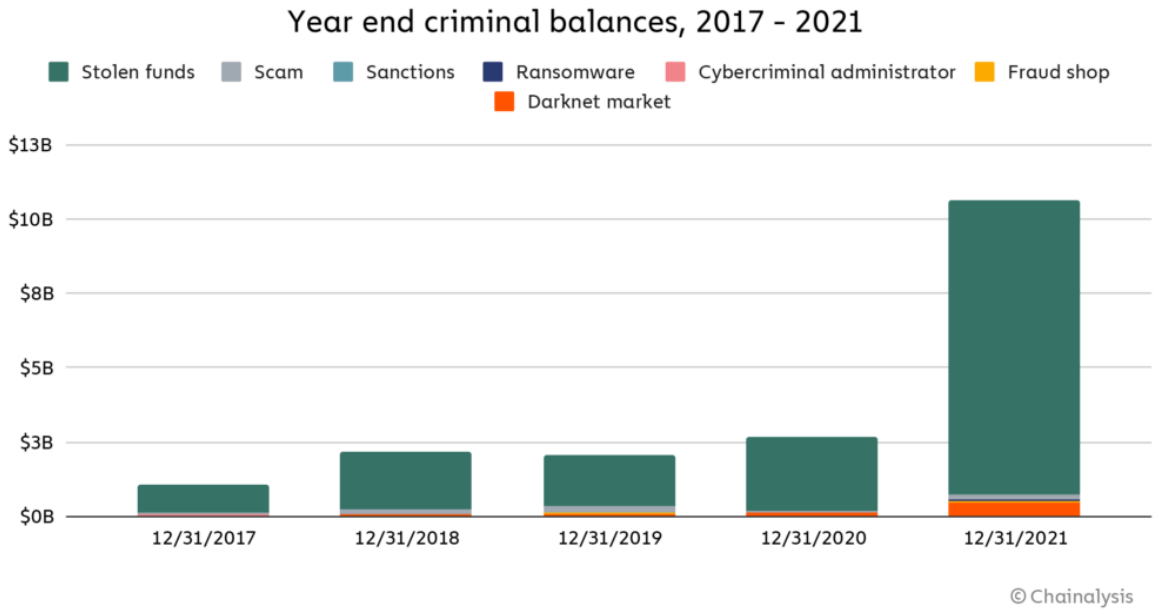
Australian data are available from the ACCC (2022), which stated that the cost of scams in Australia was over A$324 million in 2021 – a rise of 84 percent since 019 - by far the largest component being investment scams, followed by dating/romance scams and false billings. Their Scamwatch reporting system noted that Phone (voice) continued to be the most common contact method, with half of all reports and 31 percent of all losses. Text message was the second most common contact method with 23 percent of reports but more modest percentage of losses. The second highest contact method in terms of loss was social media with 17 percent of total losses. Emails represented only 14 percent of contacts but third highest source of losses. This presents a more nuanced picture of fraud and digital society. McAllister and Franks's (2021) national representative survey of identity theft in March 2021 found that 19 per cent of respondents had experienced misuse of their personal information in their lifetime and 7 per cent experienced it in the past year – a decline from 11.4 per cent in 2019. A total of 78 per cent of victims in the past year experienced a financial loss as a result. Over half found out about the ID theft only when informed by their bank. The ABS (2016) revealed that in the 12 months prior to interview in 2014–15, 8.5 per cent of the population aged 15 and over experienced personal fraud, up from 6.7 per cent in 2010–11. Over two-thirds (71 per cent) who experienced personal fraud experienced a single incident. (For a good discussion, see Emami et al., 2019.)

Cryptocurrencies and crime

The relationship between cryptocurrencies and crime is complex. In addition to the licit uses, it impacts on the supply of illicit goods and services on semi-open and dark markets, fraud on crypto-holders, market manipulation and money laundering, a process that applies to all crimes where proceeds are stored, saved and hidden or transformed (Levi and Soudijn, 2020). All of these appear to have accelerated during the COVID-19 pandemic (Bergeron et al., 2022; Buil-Gil and Saldaña-Taboada, 2022; Chainanalysis, 2022; Gundur et al., 2021; Levi and Smith, 2021), although the money laundering component of cryptocurrencies is always controversial to determine, as is the case with money laundering volumes and illicit finance flows generally (Levi, 2021; Reuter, 2013). There is little doubt that cryptocurrencies make it easier to transact on dark markets, giving the illusion of safety to vendors and purchasers, except when being run by covert law enforcement. Price fluctuations in Bitcoin and other cryptocurrencies are heavy, and whether or not (like real estate) cryptocurrency is seen – rightly or wrongly – as an investment that will almost always yield a profit over time, it is an asset that has no objective traded value. Insider knowledge ahead of price-sensitive movements in crypto can enable what would otherwise be insider trading profits. Exchanges and some wallets can be the subject of large frauds, most often by owner/managers, as shown in the figure below (which typically rises over time) (Zandt,

2022):

Cryptocurrency theft grew, with roughly $3.2 billion worth of cryptocurrency stolen in 2021 — a 516 per cent increase compared to 2020. Roughly $2.2 billion of those funds – 72 per cent of the 2021 total – were stolen from DeFi protocols (Chainanalysis, 2022: 6). Cryptocurrency-based crime hit an all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020.



However, if we take the data as a proportion of rapidly increasing crypto transactions, transactions involving identified illicit addresses represented just 0.15 per cent of cryptocurrency transaction volume in 2021, a dramatically lower percentage and a quarter of the 2020 figure. However, the proportion of cryptocurrency funds that are from criminal sources, and the proportion of total proceeds of crime that takes the form of cryptocurrency at any stage of the money laundering cycle are very different and unresolved issues, nor is there any reason to expect that they will be constant over time. Is cryptocurrency a criminological game-changer? Perhaps, as it offers better routine privacy than other media of exchange. But although tumblers and other mechanisms can make it hard to follow the ownership trail, the point of blockchain is to provide a rigorous record, and Chainalysis (2022) and others have methods of tracking. Moreover, unless it can be spent directly on things criminals want to buy, it currently has to be cashed out before it can be saved or spent easily. This is a shifting ground, as greater regulation is being introduced in the Global North countries to control the market better and reduce scams.

Digital Crimes and Policing

All fraud, whether digital or offline, is relatively difficult to police and is marked by attrition, although the extent of that attrition varies between countries and over time, depending partly on the policing resources devoted to it. Those resources have to be fought for against the range of priorities for other – usually more immediately popular – crimes, and the temperaments and skill sets of those recruited to policing (for which, see Bossler et al., 2020). In contemporary societies, many seek more effort and time spent on domestic violence, rape and ‘hate crime’. Although ‘traditional crimes’ have fallen, policing has found it difficult to adapt, and political pressures remain to focus on urban insecurity (often a code word for ethnic and religious conflicts).

Attrition should be thought about in terms of processes (including elapsed time). Specifically:

- Awareness of victimisation.
- Decisions about what to do about the experience.
- Reporting to (which?) enforcement/intelligence agency and/or civil litigation.
- Investigation (or no investigation in most cases).
- Levels of domestic and international cooperation applied for and received.
- Decision of authorities to aim for prosecution, disruption or other intervention (or No Further Action).
- Criminal trial.
- Conviction and collateral impacts.

Thus, in England in the pre-pandemic year ending March 2020, out of 403,237 police-recorded frauds, of which 36,836 had been referred for investigation, there were 5,782 judicial outcomes (Levi et al., forthcoming). Without a better understanding of the specifics of criminal investigation, it is difficult to be 'realistic', but although digital evidence sometimes leaves a better trace, it often requires assistance from private sector third parties – ISPs, card issuers and merchant acquirers, and mobile phone companies, for whom such preventative and criminal justice work is loss-making – and sometimes from countries abroad. International mutual legal assistance was designed for relatively rare cases, and with the exception of the European Union, which the UK has left, it is a clunky and laborious process, especially for those lacking detailed knowledge and the imagination to frame letters of request in the language and legal format of other countries. These problems should be eroded by electronic translation, templates and artificial intelligence. However, though non-digital frauds did require elements of these, the sheer scale of cyber-enabled and cyber-dependent crimes make it harder, even given the support of the requested law enforcement bodies and prosecutors, which has to take its place among other demands on them. One way of thinking about it is how much time does it take to process one case, and therefore given the amount of digital crime investigators available, how many such cases may be managed annually with a given set of resources.

Unsurprisingly, annual reports and other datasets do not make it easy to work out the level of this attrition. Thus, the IC3 (2010: 5) report states: 'Of the referrals prepared by the FBI analysts, 122 open investigations were reported, which resulted in 31 arrests, 6 convictions, 17 grand jury subpoenas, and 55 search/seizure warrants.' These look likely to be the same cases as 'IC3 analysts prepared 1,420 cases (representing 42,808 complaints). Law enforcement prepared 698 cases (representing 4,015 complaints)'. Thus, six convictions from 42,808 or even from 4,015 complaints would be a very modest enforcement outcome – but it can take years for cases to work their way through.

IC3 (2022) received a record number of complaints (847,376) from the American public in 2021, up more than two-thirds from 2019, with what are referred to as potential losses exceeding $6.9 billion, five times greater than in 2017. Business E-mail Compromise (BEC) schemes continued to be by far the costliest, followed byromance fraud. Phishing scams were also prominent, and ransomware cases have risen substantially over time. The IC3 (2022: 3) added:

> In 2021, the IC3's RAT initiated the Financial Fraud Kill Chain (FFKC) on 1,726 BEC complaints involving domestic to domestic transactions with potential losses of $443,448,237. A monetary hold was placed on approximately $329 million, which represents a 74% success rate.
>
> .

However, in this and previous reports, no mention was made of *final actual* asset recoveries (though these are easier in the US than elsewhere because the assets are sued physically – see Cassella, 2021), arrests, prosecutions or convictions, beyond the disconnected data discussed above and in successive annual reports.

This sort of attrition happens in every country where there has been research (Cross, 2020; Levi et al., forthcoming; Scholes, 2018). The CSEW (ONS, 2022) suggests 5 million fraud offences in England and Wales, while over approximately the same period, the central fraud-recording body Action Fraud received over 420,000 reports of digital and non-digital frauds, few of which will be investigated and even fewer brought to justice. Reports from many countries indicate how modest a resource is devoted to criminal investigation of both digital and non-digital frauds (or cyber-dependent crimes) unless they are a major threat individually to business or 'society', an exception being South Korea. This is beginning to change in the UK, with significant attacks by consumer and victim representatives and in newspapers from all sides of the political spectrum on the under-policing of (mainly consumer) frauds, but it remains to be seen whether this will result in major sustained increases in police or non-police resources, and what the impacts on different frauds of that will be.

Government and police might aim to 'satisfice' the public and victims with a not wholly scientific mix of general preventative measures (Protect), post-victim resilience (Prepare) and classic investigations (Pursue), alongside public reassurance that their concerns are being paid attention to (an important component of harm reduction omitted from the government's Four Ps), and efforts to reduce the numbers and intensity of willingness to defraud (Prevent). But issues of resourcing of these forms of digital crime management within the public and private sectors remain controversial, and shifting resources from other areas of crime control has not happened hitherto.

Discussion

A focus on cybercrime for financial gain – and indeed, on volume fraud generally – may unintentionally shift focus away a) from frauds committed by elites and others without the need for any special cyber-skills and/or b) from frauds and commercial

espionage by foreign organised or state-sponsored criminals. Where cyber-attacks are aimed internationally, then using the individual nation state as the denominator of harm, risk or threat unintentionally breaks up the collective data-integration efforts and may reduce focus on some important attack vectors and prevention/pursuit opportunities. Nevertheless, historically, national victim-centric counting has been the focus for all forms of crime, and national data are considered below.

There are other ways of looking at trends. Note, however, that threats are comprised by the motives, capacities and capabilities of attackers, as well as conscious and unselfconscious victim and third-party defensive behaviour: victim survey and reported crime data merely reflect the outcome of those routine activity 'crime triangle' activities at a point in time.

The primary focus of this chapter has been on cybercrime for financial gain (cyberfraud) against individuals, but some of these are facilitated by intentionally (with insider help) or negligently caused data breaches involving business and government records. There are now many national strategies and a large number of global, regional and national commercial victimisation surveys – mostly by vendors and financial advisory firms, but a few by governments – but there is no space to review these here. We have examined some relevant data from developed countries on trends in cyberfraud victimisation as far as they exist, using both official recorded data and victimisation surveys. Although these are not altogether comparable, it is hoped that these will be useful in considering the scale of some components of these problems in what might be termed 'human security': the national security aspects of cyberfrauds depend on how we construct that term, but negative events in trust, hacking and insider theft in commerce seep into national (in)security, making the distinction between national and human security overlap, in addition to the fact that national security is fundamentally about people who live in or are citizens of the nation.

'Threat assessments' add to the 'awareness-raising' process that may reduce substantially our risks – both probabilities and impacts – of victimisation; action (pre- and post-victimisation) increases the profits of the cybersecurity businesses that have been spawned by the rise of e-commerce and social media. In this market characterised by diverse sources of assertion, information and 'intelligence', it is difficult for most consumers, businesses, government organisations and commentators to work out a 'rational' response; and there may be significant 'market failure', as what analytical basis would the relatively or wholly inexpert have for assessing and purchasing these competing interpretations of 'solutions' to their ill-understood problems?

The emotional costs of actual cyber-related economic crimes and of the fear thereof have not been properly costed to date (Anderson et al., 2019; Levi, 2009). Some of that fear has been amplified by software sales firms and by public and private security agencies seeking more resources, but it would be too difficult to separate out these from 'true' costs. Besides, even manufactured fears become real costs for citizens, whether private individuals or businesspeople. (We should also acknowledge the paradox that many who become victims are not fearful enough, or anyway that their fears are ill-directed towards mistaken problems and solutions.)

Conclusions

This chapter deals with different dimensions of cyber-enabled crime and issues concerning the focus and the effectiveness of law enforcement responses. The activities against which they can be measured are reasonably knowable from public sources and sometimes even published. However, for others, the error margins in the data (if there are any data at all) are often too great to know whether 'the problem(s)' is getting better or worse. The relationship between levels of crime and anxiety about crime is a further important dimension that has been studied more offline than online, and more for individuals than for businesspeople. Perfect knowledge is implausible in fraud, as there will always be interpretation tensions and victim/bystander ignorance of deception: but we can and should do better in raising our understanding, not just because social harm statistics are good in themselves but also because of the need to assess the performance of crime reduction and criminal justice efforts. The national security aspects of cyber-risk are more tortuous and even harder to evaluate, but cybersecurity is in the highest category, and that somewhat opaque construct 'transnational organised crime' is in the second highest category in several national risk assessments (see ATA, 2021; Europol, 2016, 2021). In the UK National Security Risk Assessment (2021), 'Hostile attacks upon UK cyber space by other states and large scale cyber crime' is in Tier 1, 'A significant increase in the level of organised crime affecting the UK' is in Tier 2. As to the linkage between these and economic cybercrimes, it should be noted that there is not a sharp division between these larger national security issues and cyber attacks (for fraud and intellectual property theft) on banks, businesses and the spear phishing of individuals with important knowledge of system vulnerabilities in the public or the private sector. Rather, there is a punctuated continuum in the interplay between private, corporate governmental and wider social risks.

The measurement of direct and indirect intellectual property losses and even of fraud has been the subject of much dispute but in particular, the attribution of such losses to state-sponsored or state-tolerated attackers is often immensely difficult and hotly debated. As Sparrow (2008) argues, it makes a difference to our conception of harm and threat whether people are 'conscious opponents' and, by extension, what sort of conscious opponents they are. We may need to clarify conceptually the terminology that we apply to this field, a clarity that is needed in dealing with that amorphous mess of poly-criminal enterprises involved in the organisation of serious crimes (Greenfield and Paoli, 2022; Levi, 2012; van Duyne and van Dijck, 2007; von Lampe, 2016).
Finally, we might reconsider some of the overlaps that exist between online and offline crimes, and think through the ways in which online is transformative either for levels and organisation of crime commission or for the balance between disruption (another ambiguous term) and the traditional detection, investigation and prosecution processes that constitute a criminal justice response. In doing so, we should not ignore the fact that even when economic crimes were mostly or (40 years ago) entirely offline, we knew very little about their cost, incidence and prevalence, or about how effective were the modest control efforts the Global North and South made to combat some of them.

Nor should we think that anxiety about fraud is merely a feature of the rise of the internet: the Metropolitan and City of London police fraud squad was formed as a response to the risks of fraud facing those demobilised after the Second World War, and early crime surveys showed substantial anxieties about identity theft and card theft even before data breach and hacking scandals reached their recent levels (Cook et al., 2022; Levi, 2009). Measuring the impact of ICT on volume frauds is valuable, and countries that are serious about evaluating the risks that face their citizens, denizens, businesses and governments need to upgrade their statistical efforts. However, these should not be mistaken for measures of the influence of ICT on management frauds or on more general corporate crime. Whatever data we are using, our societies and law enforcement agencies need to face up to significant challenges in how to respond to the flood of cases about which – even in the comparatively well-resourced US – very little reactive enforcement follow-up normally happens and what does is often expensive and laborious to follow through. This includes responding to the crimes, promoting cyberfraud prevention and resilience, and more general 'reassurance policing'.

We cannot escape the difficulties in enhancing our awareness and getting a 'truer' picture of 'what happened' in cyber-enabled frauds – from the perspectives of offenders, victims, third parties or law enforcement. But the aim has been analogous to that of Becker (1974) in his needlessly apologetic comments in his reconsideration of labelling theory: 'a perspective whose value will appear, if at all, in increased understanding of things formerly obscure'.

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T. and Savage, S. (2012) 'Measuring the cost of cybercrime'. Available at: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T. and Vlasek, M. (2019) 'Measuring the changing cost of cybercrime'. Available at: https://informationsecurity.uibk.ac.at/pdfs/ABBCGGLMV2019_Measuring_the_Changing_Cost_of_Cybercrime_WEIS.pdf

ATA (2021) *Annual Threat Assessment of the Intelligence Community, 2021*. Office of the Director of National Intelligence, Washington, DC.

Balleisen, E. (2018) *Fraud: An American History from Barnum to Madoff*. Princeton, NJ: Princeton University Press.

Barnett, C. (2002) 'The measurement of white-collar crime using uniform crime reporting (UCR) data'. Available at: https://ucr.fbi.gov/nibrs/nibrs_wcc.pdf

Beck, U. (1992) *Risk Society: Towards a New Modernity*. Thousand Oaks, CA: Sage.

Becker, H. (1974) Labelling Theory Reconsidered: Deviance and Social Control. London: Tavistock. pp. 4166.

Bergeron, A., Décary-Hétu, D., Giommoni, L. and Villeneuve-Dubuc, M.P. (2022) 'The success rate of online illicit drug transactions during a global pandemic', *International Journal of Drug Policy*, 99: 103452.

Bossler, A. M., Holt, T.J., Cross, C. and Burruss, G.W. (2020) 'Policing fraud in England and Wales: Examining constables' and sergeants' online fraud preparedness', *Security Journal*, 33 (2): 311–28.

Buil-Gil, D. and Saldaña-Taboada, P. (2021) 'Offending concentration on the internet: An exploratory analysis of bitcoin-related cybercrime', *Deviant Behavior*, 1–18.

Cassella, S. (2021) *Asset Forfeiture Law in the United States*(3rd edn), Huntingdon, PA: Juris.

Chainanalysis (2022) *The 2022 Crypto Crime Report*. Available at: https://go.chainalysis.com/2022-Crypto-Crime-Report.html

Cook, S., Giommoni, L., Trajtenberg, N., Levi, M. and Williams, M. (2022) 'Fear of economic cybercrime across Europe: A multilevel application of Routine Activity Theory', *British Journal of Criminology*.

Cross, C. (2020) 'Reflections on the reporting of fraud in Australia', *Policing: An International Journal*, 43 (1): 49–61.

Domenic, M., Leukfeldt, E., van Wilsem, J., Jansen, J. and Stol, W. (2013) *Victimisation in a Digitised Society*. The Hague: Eleven International Publishing.

Dodsworth, L. (2021) *A State of Fear: How the UK government weaponised fear during the Covid-19 pandemic*. London: Pinter & Martin.

Dutch Safety Monitor (2022). *Safety Monitor 2021*. www.cbs.nl/nl-nl/longread/rapportages/2022/veiligheidsmonitor-2021?onepage=true

ECB (2021) *Seventh Report on Card Fraud*. Frankfurt: European Central Bank.

Elison, A. (2022) "Banks return less than half of cash lost to fraud despite pledge", *The Times*, March 09,

Emami, C., Smith, R. G. and Jorna, P. (2019) *Online Fraud Victimisation in Australia: Risks and Protective Factors* (No. AIC Research Report 16). Australian Institute of Criminology, Canberra.

Europol (2016) *IOCTA 2016: Internet Organised Crime Threat Assessment*. The Hague: Europol.

Europol (2021) *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Publications Office of the European Union, Luxembourg.

Eurostat (2015) *Special Eurobarometer 423: Cybersecurity Report*. Available at: https://op.europa.eu/en/publication-detail/-/publication/910d76f6-0c77-4ea6-b9eb-fd854fc6c3ac/language-en

Eurostat (2019) *Special Eurobarometer 499: Europeans' Attitudes Towards Cyber Security (Cybercrime)*. Available at: https://europa.eu/eurobarometer/surveys/detail/2249

Felson, M. (2003) 'The process of co-offending', in M. Smith and D. Cornish (eds), *Theory for Practice in Situational Crime Prevention, Crime Prevention Studies*, 16: 149–67. Mounsey, NJ: Criminal Justice Press.

FTC (2022) *Consumer Sentinel Network Data Book 2021*. Available at: www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf

Gee, J. and Button, M. (2019). *The Financial Cost of Fraud 2019*. Available at: www.crowe.ie/wp-content/uploads/2019/08/The-Financial-Cost-of-Fraud-2019.pdf

Greenfield, V. and Paoli, L. (2022). *Assessing the Harms of Crime: A New Framework for Criminal Policy*. Oxford: Oxford University Press.

Harrell, E. (2021) 'Victims of identity theft, 2018'. Washington DC: Government Printing Office. Available at: www.bjs.gov/content/pub/pdf/vit18.pdf

IC3 (2010) *2010 Internet Crime Report*. Internet Crime Complaint Center.

IC3 (2022) *2021 Internet Crime Report*. Internet Crime Complaint Center.

Kloosterman, R. (2015) 'Slachtofferschap cybercrime en internetgebruik', *Sociaaleconomische trends*, 9: 1–18.

Leger (2016) Financial Fraud Survey. Montreal: Select PR/Equifax.

Leukfeldt, E.R., Kleemans, E.R. and Stol, W.P. (2017) 'Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks', *The British Journal of Criminology*, 57 (3): 704–22.

Levi, M. (2008a) *The Phantom Capitalists: the Organisation and Control of Long-Firm Fraud* (2nd edn). Andover: Ashgate.

Levi, M. (2008b) '"Organised fraud": Unpacking research on networks and organisation', *Criminology and Criminal Justice*, 8 (4): 389–420.

Levi, M. (2008c) 'White-collar, organised and cyber crimes in the media: some contrasts and similarities', *Crime, Law and Social Change*, 49: 365–77.

Levi, M. (2009) 'Fear of fraud and fear of crime: A review,' in S. Simpson and D. Weisburd (eds), *The Criminology of White-Collar Crime*. New York: Springer.

Levi, M. (2012) 'The organisation of serious crimes for gain', in M. Maguire, R. Morgan and R. Reiner (eds) *The Oxford Handbook of Criminology* (5th edn).Oxford: Oxford University Press. pp. 595–622.

Levi, M. (2021) 'Evaluating the control of money laundering and its underlying offences: The search for meaningful data', *Asian Journal of Criminology*¸ 15 (4): 301–20.

Levi, M. and Burrows, J. (2008) 'Measuring the impact of fraud: A conceptual and empirical journey, *British Journal of Criminology*, 48 (3): 293–318.

Levi, M. and Smith, R. (2021) *Fraud and its Relationship to Pandemics and Economic Crises: From Spanish Flu to COVID-19*. Research Report No. 19. Australian Institute of Criminology, Canberra. Available at: www.aic.gov.au/publications/rr/rr19

Levi, M. and Soudijn, M. (2020) 'Understanding the laundering of organized crime money', in P. Reuter and M Tonry (eds) *Organizing Crime: Mafias, Markets, and Networks*, *Crime and Justice: an Annual Review of Research*, 49: 579–631.

Levi, M., Doig, A., Luker, J., Williams, M., and Shepherd, J. (forthcoming) *A Public Health Approach to Fraud*, West Midlands Police and Crime Commissioner.

Lusthaus, J. (2018) *Industry of Anonymity: Inside the Business of Cybercrime*. Cambridge, MA: Harvard University Press.

Lusthaus, J., Van Oss, J. and Amann, P. (2022) 'The Gozi group: A criminal firm in cyberspace?'. *European Journal of Criminology*, 14773708221077615.

McAlister, M. and Franks, C. (2021) *Identity Crime and Misuse in Australia: Results of the 2021 Online Survey* (No. AIC Statistical Bulletin 37). Australian Institute of Criminology, Canberra.

Morgan, R. (2021) *Financial Fraud in the United States, 2017*. Washington, DC: Goverment Printing Office.

NAS (2016) *Modernizing Crime Statistics: Report 1: Defining and Classifying Crime*. National Academies of Sciences, Engineering, and Medicine. Washington, DC: The National Academies Press. Available at: https://doi.org/10.17226/23492

ONS (2022) *Crime in England and Wales: Year Ending September 2021*. Available at: www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2021#fraud

Scholes, A. (2018) *The Scale and Drivers of Attrition in Reported Fraud and Cyber Crime*, Research Report 97. London: Home Office.

Sparrow, M. (2008) *The Character of Harms*. Cambridge, MA: Harvard University Press.

Statistics Canada (2011) *Self-reported Internet Victimization in Canada, 2009*. Ottawa: Statistics Canada.

UK National Security Risk Assessment 2021 (2021) *Factsheet 2*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62484/Factsheet2-National-Security-Risk-Assessment.pdf

Van Duyne, P.C. and Van Dijck, M. (2007) 'Assessing organised crime: The sad state of an impossible art', in F. Bovenkerk and M. Levi (eds) *The Organized Crime Community*. New York: Springer: pp. 101–24.

Von Lampe, K. (2016) Organized Crime: Analyzing Illegal Activities, Criminal Structures, and Extra-legal Governance. Thousand Oaks, CA: Sage.

Wall, D.S. (2007) *Cyber Crime*. Cambridge: Polity Press.

Wallis, N. (2021) *The Great Post Office Scandal*. Bath: Bath Publishing.

Which? (2021) *Scams and Subjective Wellbeing: Evidence from the Crime Survey for England and Wales*, Which? and Simetrica-Jacobs.

Whitty, M.T. (2018) '419 – It's just a game: Pathways to cyber-fraud criminality emanating from West Africa', *International Journal of Cyber Criminology*.

Wilson, S. (2014) *The Origins of Modern Financial Crime: Historical Foundations and Current Problems in Britain*. London: Routledge.

Zandt, F. 2022. *The Biggest Crypto Heists*. *Statista*. New York: Statista Inc. www.statista.com/chart/12707/largest-known-crypto-currency-thefts/ Accessed 27 July 2022.