Assessing the trends, scale and nature of economic cybercrimes

Michael Levi, Professor of Criminology, School of Social Sciences, Cardiff University, CF10 3WT[1]

In Cybercrimes, Cybercriminals and Their Policing, in *Crime, Law and Social Change*

DOI: 10.1007/s10611-016-9645-3

Abstract

Trends in police-recorded and (where they exist) household survey-measured cybercrimes for economic gain are reviewed in a range of developed countries – Australia, Canada, Germany, Hong Kong, the Netherlands, Sweden, the UK and the US - and their implications for criminal policy are considered. The datasets indicate a substantial rise in online fraud – though one that is lower than the rise in online shopping and other 'routine activity' indicators - but it is not obvious whether this is just displacement for the fall in household and automobile property crime, nor how much overlap there is between the offenders and past 'offline' offenders. Nor do the data indicate whether the frauds result from insiders or outsiders, or are collusive. The direct and indirect costs of cyberfrauds are examined, and it is concluded that there is no satisfactory basis for the larger estimates of cost, but it is undeniable that those costs are large enough to merit concern. There remains a problem of what metrics are appropriate for judging the threat and harm from cybercrimes, and their impact on national and human security. There is not a sharp division between these larger national security issues and cyber attacks 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.

Keywords

Cybercrime; fraud; global trends; cost; harm; national security; human security; routine activities.

Introduction

When the late Ulrich Beck (1992) coined the term 'risk society', his focus was not on the salience of this concept to crime. Since then, it appears that risks and threats to current and future processes in the 'cyber' world are everywhere (as they are to other – usually mainly offline – crime arenas such as money laundering, transnational organised crime and, above all, terrorism). 'Threat assessments' add to the 'awareness-raising' process that is currently (always?) insufficient to eliminate or 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?

[1] Levi@Cardiff.ac.uk

This is far from being a unique issue in criminology. After all, academics have been discussing for decades the disparity between real victimisation rates and public beliefs about the incidence, prevalence and forms of particular crimes (like another heterogeneous category, 'violent crime'). However, data availability in the sphere of both recorded and unreported cyber-related crimes has been poor, and suspicions about both the motivations and the accuracy of third party cybercrime data producers have surfaced periodically (see Anderson et al. (2012) for a review of cost of cybercrime data; and Levi and Burrows (2008) for an earlier review of the cost of fraud in the UK). Apart from country-specific surveys, the Eurobarometer delivers the only cross-national comparative data collection on fraud victimization in the EU (see http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf.), showing clear variation in identity theft between countries. Although Williams (2016) provided some evidence that - when combined with individual level cyber security - national cyber security strategies have some measurable effect upon victimisation,[2] both evidence of actual risk and knowledge of 'what works' in cybercrime reduction against individuals, business and governments are much in dispute.

It has been alleged that the UK government was suppressing the rise in fraud and cybercrime, falsely claiming success in 'crime reduction' when in fact there might simply have been a displacement from better measured offline to ill-measured online crimes, whether committed for financial gain or (not dealt with in this article) of harassment and psychological gain for offenders/harm to victims (The Guardian, 2013; Fitzgerald, 2014). It is also possible that a focus on cybercrime for financial gain – and indeed, on volume fraud generally – may 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. One – conventional in cybersecurity circles and in regular vendor and consultancy reports on risks – is to look at evolving techniques of cyber attacks and the 'threat landscapes': see, for example, the Europol iOCTA and ENISA reports.[3] There are many such products and articles, which are important to prevention and to cybersecurity – indeed, business reporting of critical infrastructure cyberattacks is mandated by the 2013 European Directive on attacks against information systems, though such reports will be to bodies like CERTs and CISPs rather than to the police. However, there is little added value in repeating these here, and because patterns and rates of change of victimisation (and sensational cases) tend to drive police and government crime policies, a more classical approach has been adopted in this article. Note, however, that threats are comprised by the motives and capabilities of attackers, as well as

[2] See further, http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf.

[3] The author is a member of the Europol iOCTA and SOCTA advisory groups.

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 article is on cybercrime for financial gain (cyberfraud) against individuals – discussed in greater detail in Levi et al. (2015) and by Levi et al. in this volume, 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 (see Levi et al., 2015 for a partial review, though new material emerges regularly). Below are 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.

In those jurisdictions such as Germany where the financial losses to police-recorded crime are calculated, fraud greatly outstripped losses in other acquisitive crimes, but the breakdown of losses into cyber-enabled/other is not available. However, 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.

Trends in recorded and survey measured cyberfrauds

The Eurobarometer (Eurostat, 2015) reports that in 2014, the proportion of Internet users experiencing online fraud (12% on average across the EU) is similar in most EU countries: the highest figure can be found in Poland (19%), and the lowest are Greece (4%) and Bulgaria (6%). As for identity theft, on average across the EU, 7% of Internet users say they have experienced or been a victim. This figure is similar in most EU countries, although respondents in Hungary and Romania (11%) are more likely and those in Bulgaria and the Netherlands (both 3%) are least likely to be victims. The largest increases since 2013 can be found in Romania (up 6 percentage points) and France (up 5 points), while the largest decrease can be seen in Malta (down 6 points).

The United Kingdom

The response to these criticisms in England and Wales has been an acceleration of attempts by the Office of National Statistics (ONS) and by the Home Office to improve fraud and cybercrime statistics, adding them to both official crime statistics and crime surveys against individuals and businesses. (Though such changes are made warily, since they generate a massive rise in officially

recognised crime and a significant change in the time series of crime statistics, which has to be explained to a suspicious media and public often looking for political massage in data, even in changes which make 'government effectiveness' look worse[4]: early iterations are therefore explicitly described as 'experimental statistics', ONS, 2016a, b).

Findings from a 2015 field trial were refined into a revised crime survey, and the first wave of experimental statistics showed that in the year ending March 2016, adults aged 16 and over experienced an estimated 3.8 million incidents of fraud, with just over half of these being cyber-related.[5] The most common types of fraud experienced were "Bank and credit account" fraud (66% of all incidents), followed by "Non-investment" fraud – such as fraud related to online shopping or fraudulent computer service calls (28% of incidents). In addition, adults experienced an estimated 2.0 million computer misuse incidents; around two-thirds of these were computer virus related and around one-third were related to unauthorised access to personal information (including hacking). Data show that 4.7 percent of adults were victims of payment card fraud, but do not provide any information on the number of times such frauds occurred or the scale of any loss that may have been experienced (ONS, 2016a). The accompanying note on fraud generally (ONS, 2016b) illuminates with greater details and methodology, but I would add that though the Action Fraud reports include a variety of frauds (see ONS, 2016b and Levi et al. in this volume), neither they nor the household or commercial victimisation surveys have much to say about the sort of high seriousness cases dealt with in the UK by the Serious Fraud Office or the tax frauds handled by the Specialist Fraud Division of the Crown Prosecution Service, whose total financial value dwarfs the volume fraud cases discussed here. The cyber component in such cases has not been examined in detail but is usually present to some degree, as authorised financial transfers normally occur electronically. Thus, while many major frauds generate false data electronically (such as the Madoff Ponzi scheme fictitious securities records showing investment profits), the ICT merely facilitates the scale of these crimes, especially where there are large numbers of victims.

The crime survey data (ONS, 2016b) reveal that:

- The large majority of victims of fraud had been a victim only once (84%), although repeat victimisation (within the same 12 month crime reference period) was more common among victims of bank and credit account fraud (14%) than among victims of other types of fraud.
- Almost two-thirds of fraud incidents involved initial loss of money or goods to the victim (62%), independent of any reimbursement received.

[4] The author must declare an interest, as an independent member of the UK Statistics Commission's Crime Statistics Advisory Committee, and a member of Europol's Internet-related Organised Crime Threat Assessment Advisory Group.

[5] Reyns (2013) connects BCS 2008/9 data on identity fraud to routine activity indicators, showing higher risk for high-income households and people active online.

- Victims received a full reimbursement in 43% of fraud incidents (1.6 million), typically from their financial provider. However, in 690,000 cases, the victim received no or only partial reimbursement.
- Where money was taken or stolen from the victim, in just under two-thirds of incidents the victim lost less than £250 (64%).
- Incidents of bank and credit account fraud were more likely than other types of fraud to result in initial loss to the victim (70%, equivalent to 1.7 million). The victim received a full reimbursement of their direct financial losses in 84% of cases.[6]
- In 49% of non-investment frauds (such as fraud related to online shopping scams or fraudulent computer service calls) and 76% of all other frauds (for example, lottery scams, pyramid or Ponzi schemes or charity fraud) there was no loss to the victim. This compares to 30% of incidents of bank and credit account fraud where no loss was suffered.
- With regard to computer misuse, 22% of incidents involved loss of money or goods, all relating to computer viruses (442,000 incidents). This would include malware extortion.

Complete time series of all offences cannot be reconstructed. However, on-line frauds have risen over time, except for those affected by the introduction of Chip and PIN onto payment card transactions, which have fallen significantly in the UK and elsewhere, despite being displaced somewhat to the US where Chip and PIN have only recently and gradually been implemented (ECB, 2015; FFA UK, 2016a). These technological changes have in a sense reduced ICT-enabled frauds, namely the widespread copying of magnetic stripe data onto blank or other payment cards. Thus now, remote purchase frauds constitute 70% of all bank payment card fraud – almost doubling since 2011 to £398.2 million in 2015, with a further 7% being identity frauds; remote banking fraud has more than doubled since 2011, now totalling £168.6 million (FFAUK, 2016b). It is unwise and incorrect to demarcate hermetically online from offline crimes: combined email and telephone-based social engineering methods have become very common in inducing people to transfer funds to fraudsters, sometimes inducing victims to deliver large sums in cash to couriers who call at their homes.[7]

The proportion of Action Fraud cases that are cyber-enabled is unknown, but reports from the public to Action Fraud were affected by the disruption caused by the financial failure of the previous call centre. Most of the increase in "banking and credit industry fraud" is thought to have resulted from

[6] This is a somewhat contentious area, as alleged victim negligence (for example in writing down their PIN or giving it to someone else for convenience) can be a reason for refusal of reimbursement which is defended by the banks but resented by cardholders and contested by some academic critics of bank processes.

[7] This has been the subject of several radio consumer programmes and City of London police warnings. To include the telephone in an aggregated count of ICT may be unhelpful: the fraudsters may have used VOIP (Voice Over Internet Protocol) to reduce criminal running costs and traceability. But it is harder to disguise sex, age and ethnicity if there is human communication compared with email and text.

an increase in the volume of reported identity frauds in account applications (for example, applying to open a payment card account using a false identity). Since most of these are opened online, these are cyber-enabled or at least cyber-assisted.

Scotland is a separate jurisdiction and has many separate criminal offences. It is currently (June 2016) considering the measurement improvements in England and Wales, but the most recent data available are from 2014/15. 5% of adults had experienced card fraud in the 12 months prior to interview (an average of 1.4 times), up from 4% the previous year. In both years, 1% of adults had been victims of identity theft, where someone had pretended to be them or used their personal details fraudulently (Scottish Government, 2014, 2016). Though the report does not make this point, this would make fraud the most common type of acquisitive crime in Scotland, as well as being a prime cause of anxiety about crime. In 2014/5, the crimes that the largest proportion of Scots adults were worried or very worried about were that someone would use their credit card or bank details for fraud (54%) or that their identity would be stolen (45%); and these were also the offences that they thought were most likely to happen to them in the next year (17% and 11% respectively).

There have been cybercrime reduction efforts and a national resilience strategy in Scotland (discussed in another article in this volume and http://www.gov.scot/Publications/2015/11/2023/3). Police-recorded crimes there show that in the period 2005-15, over 220 cases of unauthorised access and (or) causing damage/impairment to a computer/network were recorded by the police in Scotland. Where reported to the police, crimes identified as cyber-enabled will be recorded under the specific offence code for the registered crime (for example fraud, including online banking fraud and mass marketing fraud, and thefts such as using technology to steal personal data). Whilst the legacy force data did not record the use of a computer to perpetrate these crimes in a searchable format, Police Scotland's IT system (and that in the rest of the UK) aims to include a 'cybercrime' marker that will be able to provide a more accurate understanding of where there has been a cyber element to a reported/recorded crime. The data also show (http://www.gov.scot/Publications/2015/09/5338/318201)

> "Crimes of Fraud account for 5% of Crimes of dishonesty. Over the ten year period from 2005-06 to 2014-15, this category has fluctuated but overall has seen a decrease of 38%, and has decreased by 15% between 2013-14 and 2014-15."

But this tells us nothing about the true situation of either fraud or cybercrimes generally there, upon which subject the reports remain silent.

Germany

According to the Police Crime Statistics (PCS) the average number of cybercrime offences for Germany is significantly smaller in the year 2014 than it was in previous years, whereas the clear-up rate increased in the same period. The German Federal Report (2015: 4) states that these result from changes in recording rules: Up until the end of 2013, the majority of the Länder (regions) recorded cybercrime offences as having caused damage in Germany (a computer harmed by

malware or a fraud victim based in Germany, for example) even if it was not known if the criminal act had been committed in Germany or abroad. In 2014, they would be recorded only where there are concrete indications that the criminal act was committed in Germany. Thus the drop in recorded computer crime from 88,722 in 2013 to 73,907 in 2014 does not represent a real fall. Prior to these, the statistics for computer fraud did not show any major increases, but computer crime had done, but not extravagantly (from 62,944 in 2007). Recorded frauds that can be connected to cyber are rising, e.g. in 2014, the Bundeskriminalamt registered an increase of 70.5% in cases of Phishing directly related to online-banking (6,984 cases).

The Netherlands

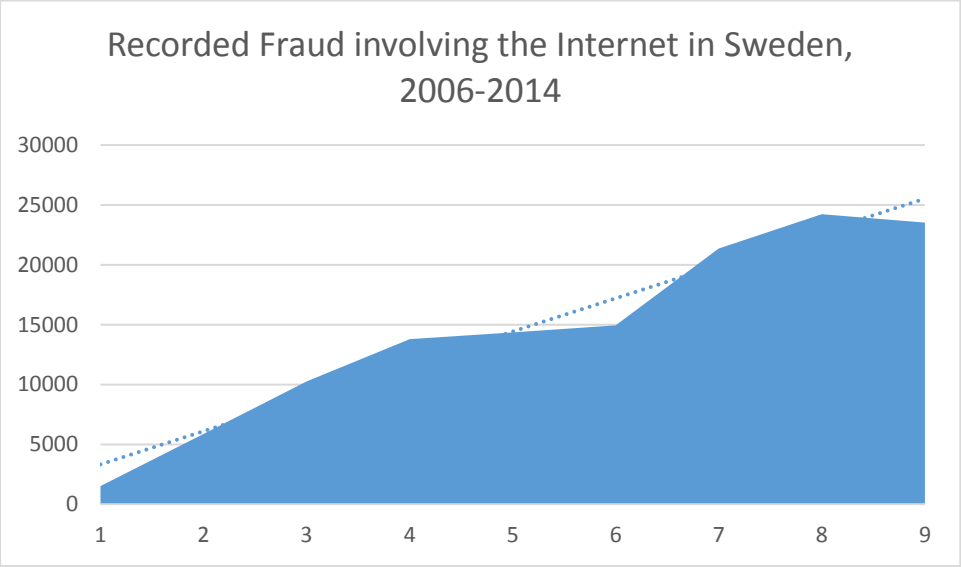
A one-off Dutch study in 2011 (Domenic et al., 2013) showed that of those using auction sites, 3.4% were victimized by some version of auction fraud. Less than 1% of the respondents had been victimized by identity fraud on the Internet, but among that group, certain Internet practices, like participating in pay contact or dating sites, seem to contribute to the chances of being victimized through Internet identity fraud.[8] A later 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 percent of the population, followed by acquisitions and sales fraud (3.5 percent) and identity theft (less than 1 percent). Compared with 2012, there were fewer victims of hacking and identity theft, but more share telemarketing fraud victims. Online shopping fraud has increased from 2.7 percent in 2012 to 3.3 percent in 2014, outstripping the rise in the percentage who shopped online. 5.8 percent of those who shopped online were victims of online shopping fraud, up from 5.3 percent in 2012. Rates of reporting to the police were low, the most common being for online shopping frauds, where a quarter reported to the police. The LISS panel data indicated that for identity fraud, 10% of the frauds were reported to the police, and they tended to be a selective group with a much higher than average financial loss. The Dutch Safety Monitor noted that in 2015, 11.1 percent of the Dutch population indicated they had been victims of one or more cybercrime offenses, ranging from identity theft and online shopping fraud to hacking and cyber bullying. 0.6 percent of the Dutch population fell victim of identity fraud, but some were repeat victims: one identity fraud *incident* occurred per 100 inhabitants. In 2015, 3.5 percent of the Dutch population reported they had been scammed while buying or selling goods or services online: about the same as in 2014. There is little repeat victimization in cases involving sales or purchase scams.

The cost of identity fraud in the Netherlands was estimated at 147-248 million euros in 2008-2009 and between 134-228 million euros in 2010-2012, according to LISS panel results on victimization and financial harm. These numbers are based on questions posed to victims on the amount of money that was illegally withdrawn from their bank accounts (Paulissen and van Wilsem, 2015).

[8] see also van Wilsem's (2013a, b) representative household panel, so more people per household are allowed to participate. It is smaller than the Domenic survey, but it is a longitudinal sample. Specific online behaviours predicted specific online victimization types (e.g., using social media predicted only harassment and not hacking).

Sweden

The Swedish Crime Survey 2014 shows that the percentage of people exposed to fraud has gradually increased from 2.5 per cent in 2006 to 3.5 per cent in 2013 before falling to 3.1 percent in 2014, and 44 percent of these involved the Internet. The only acquisitive crime more common than fraud in Sweden is bicycle theft. 84 percent 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 victims). Median losses are under 10,000 Kroner (£817/$1,171). In terms of recorded fraud, compared with 2013, Computer Fraud increased by 25 percent to 42,900 reported crimes. See further, https://www.bra.se/bra/brott-och-statistik/bedragerier-och-ekobrott.html. The trend in recorded data may be seen below:



Switzerland

Like other jurisdictions, Switzerland has been experiencing a rise in reported e-Crimes, rising from 6,181 offences in 2010 to 10,214 in 2014, with a rising proportion of those being property offences (Cybercrime Coordination Unit Switzerland, 2015). The Swiss component of the International Crime Victimisation Survey showed a drop from 2010 to 2015 in the proportion who were victims of online shopping frauds, from 41.8 to 28.6%; and in payment card fraud, from 1% in 2009 to 0.4% in 2015 (Biberstein et al., 2016).

Australia

The ABS (2016) national personal fraud survey revealed that in the 12 months prior to interview in 2014-15, an estimated 1.6 million Australians experienced personal fraud, i.e. 8.5% of the population aged 15 and over, up from 6.7% in 2010-11. Over two thirds (71%) who experienced personal fraud experienced a single incident. Three-quarters of persons who experienced personal fraud incurred a financial loss. The total estimated financial loss as a result of all personal fraud incidents was $3 billion dollars.

The most common fraud type was card fraud, affecting 5.9% of the population aged 15 and over, compared with 3.7% in 2010-11. The total estimated financial loss to card fraud in 2014-15 was $2.1 billion, double the losses in 2010-11. However, the financial loss after reimbursement (out of pocket loss) decreased between 2010-11 and 2014-15, from $208.9 million to $84.8 million, showing the importance of compensation rules and public pressure in allocating the distribution of losses between banks and the public.

0.7% of the population aged 15 and over were victims of identity theft. No fewer than 56% of the Australian population 15 or over was exposed to at least one type of scam, and of those exposed, 4% admitted responding (though this total of actual victims was lower than in 2010-11, showing the importance of crime reduction measures in reducing actual vulnerability).

The United States

The US has long been notorious for the inadequacy of its national recorded fraud statistics. Thus while we have detailed data on bank robberies, there is no real white-collar crime count: it is as if the nation was stuck in the Dillinger Days of the early1930s, when inter-state robberies were the primary risk. Nevertheless, a broader search shows that the FBI's Internet Crime Complaints Center (IC3) does collect centrally individual crime complaints for internet frauds, though for reasons that are hard to understand conceptually, these are not included in the Uniform Crime Reports or integrated in other crime counts. In 2015, the IC3 received 288,012 complaints (up from 269,422 the previous year) with an adjusted gross dollar loss of $1,070,711,522 (up from $800.5 m. in 2014); the average loss for those reporting loss was $8,421; and the median dollar loss was $560 (FBI, 2015, 2016). The total losses therefore are substantial, but would not be a large proportion of the cost of white-collar and corporate crime generally, though the latter have not been precisely analysed. The peak year was 2011, when 314,246 complaints were received. The IC3 estimates that fewer than 10 percent of victims file directly through ww.ic3.gov, but the basis for this estimate is not disclosed. The unit contributed to the efforts of combating Internet crime by disseminating over 1,500 referrals to law enforcement agencies in 2014, of which many referral packages included multiple complaints. In 2015, the corresponding data were not provided. But it provided 165 referrals to eight Cyber Task Forces, which opened 39 Operation Well Spring investigations involving some 3,650 individual complaints, with a total victim loss of approximately $55 million (FBI, 2016). As is common everywhere, at least in the public arena, there is no systematic follow up of what happens to those reports, and there is little insight into the subsequent case attrition (or disruption) process.

What this amounts to is that fraud, particularly identity theft, has become the modal acquisitive crime by volume in the US (and in other advanced Western economies), as other property crimes have fallen, and that the percentage of people suffering (or aware of suffering) identity theft has risen over time. (See Tcherni et al., 2016 for a helpful discussion based largely on US data; and Harrell, 2015, for the most recent US identity theft survey, which shows *inter* alia that about 7% of persons 16 or older were victims of identity theft in 2014, similar to findings in 2012; and the number of 'elderly' victims of identity theft increased from 2.1 million in 2012 to 2.6 million in 2014.)

Canada

53 percent of Canadians have been the victims of financial fraud in their lifetimes (Leger, 2016). This includes 34% who have been victims of unauthorised payment card fraud, and a quarter experiencing phishing emails (defined as an *attempt* to acquire sensitive information such as usernames, passwords credit card details – personal communication with Leger). 12% have been victims of telephone scams, and 4% of identity theft.

An Internet victimization survey in 2009 found that about 4% of Canadians who used the Internet in the previous 12 months reported being the victim of bank fraud on the Internet (Canada Statistics 2011). People living in cities were twice as likely as others to report internet bank fraud. About 14% of Internet users who made online purchases in the 12 months preceding the survey encountered problems, most often not receiving goods or services that had already been paid for, receiving goods or services that were not as described on the website or having extra funds taken from their account.

Two-thirds (65%) of Internet users reported that their computer had been previously infected by a virus, spyware or adware (although this does not mean that any economic harm resulted from this). Another 4 in 10 Internet users (39%) indicated that they had experienced at least one phishing attempt. Unfortunately, the Canadian government has not repeated these questions in its crime surveys. Reyns & Henson (2016) report that 3% of Canadians were victims of identity theft in 2009, and that there was a significant relationship between online activity and victimization risk. They cite figures from Statistics Canada that in 2011, identity-related crimes occurred at rates of 11.5 (identity theft) and 22.9 (identity fraud) per 100,000 persons, respectively.

The above countries are those where there has been some significant attempt at official measurement of victimisation beyond police-recorded crime data. However, there are other important countries – some with high technological development – which have not done so, and some examples are set out below.

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.

Number of cases and the financial losses due to reported computer crime in Hong Kong

Year	No. of Cases	Financial Loss (HK$ million)
2015	6862	1828.90
2014	6778	1200.68
2013	5133	916.90
2012	3015	340.41
2011	2206	148.52
2010	1643	60.38
2009	1506	45.10

Source: Hong Kong Police Force - http://www.infosec.gov.hk/english/crime/statistics.html

According to the Hong Kong Monetary Authority, there are 11 million online banking accounts in the city, which generated 17 million transactions worth HK$7.3 trillion per month in 2015.

The upwards trend in cases may also be seen in the other highly technologized countries of South Asia and South East Asia such as the Republic of Korea (where reported computer crimes have doubled since 2004); in Singapore, which has seen a trebling in reported cases of online cheating since 2013; and in India, where the number of cases registered by the police under the Information Technology Act grew by more than 50% in both 2012 & 2013 from 2011. The cases registered under the Indian Penal Code in 2013 more than doubled from 2012 (https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/). Given the rise in the use of technology for shopping and dating, the rise in the number of recorded cases is substantially less than the volume of transactions, and given that confidence in the police is so variable and/or unresearched in many countries, these data might be considered alongside the global surveys by such as McAfee Labs, Trend Micro, and PwC.

Costs and Impact of Cyberfraud

Public policy on cybercrimes often uses politically convenient data and/or data that have not been properly considered, and the appropriate metrics remain disputed (Graves et al., 2016; Jardine, 2015). Alternatively, one might consider frauds (and other crimes) as a ratio of routine activities, including internet shopping and mobile phone banking which has increase dramatically in the UK (BBA, 2016a) and elsewhere, even in developing countries. A sub-set of those costs are those of cyberfrauds, whose costs are and should always remain an area of contested argument. Efforts at cost estimation will always be provisional, not least because the exploitation of vulnerabilities and

collateral damage may take years (if ever) to emerge: the 'tail' of costs from a data breach, for example, may depend on the organisation of crimes, the responses of victims and third parties, etcetera. The UK Home Office has embarked upon work on the costs of cyber crimes but data are not available at this stage. No study of the costs of cybercrime can be definitive, even as a snapshot in time, let alone as 'data' to be used by politicians in perpetuity, as the widely disparaged Detica (2011) £27 billion 'estimate' for the UK has been. It has become common for national cybercrime strategies to cite other countries' work, only sometimes (as in the New Zealand 2015 one) with appropriate caveats of comparability. The spectrum is between a narrow summation of the known direct costs of detected crimes (perhaps even restricted to cases where a conviction has been obtained, because only then is criminality definitive), at one end, and speculative extrapolations from cases or sub-sets the dimensions of whose sets are unknown, at the other. In cyber, this is particularly complicated because it is a set of diverse acts representing mechanisms of crime commission, about which few organisations - whether victims or third parties like the police or vendors - compile data comprehensively or systematically. And unlike fraud (at least in the UK), relatively little systematic effort has gone into measuring the costs of any sub-component of 'the cyber problem'.

The emotional costs of actual cyber-related economic crimes and of the fear thereof have not been properly costed to date (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.)

For each of the main categories of cybercrime, Anderson et al. (2012) set out what is and is not known of the direct costs, indirect costs and defence costs – both to the UK and to the world as a whole, since the attribution of costs to particular countries is especially difficult in cyber. With global estimates, some fairly crude scaling based on GDP or in some cases, volumes of internet trade, have to be done to estimate costs to particular countries. Since the means (e. g., botnets) would not be around if there were not ends (e. g., phishing victims), we consider losses caused by the cybercriminal infrastructure as indirect by nature; irrespective of whether or not the legal framework formally criminalizes the means. Anderson et al. were more cautious than many others about the costs of IP espionage, since so little is known about both losses and whether external cyber-attacks or (as we suspect) internal corruption/protest/ disloyalty – depending on one's ideological position as well as on the evidence- are the primary cause of those that we do know about.

We distinguished carefully between traditional crimes that are now 'cyber' because they are conducted online (such as tax and welfare fraud); transitional crimes whose modus operandi has changed substantially as a result of the move online (such as credit card fraud); new crimes that owe their existence to the Internet; and what we might call platform crimes such as the provision of botnets which facilitate other crimes rather than being used to extract money from victims directly.

As far as direct costs are concerned, we found that traditional offences such as tax and welfare fraud cost the typical citizen in the low hundreds of pounds/ Euros/ dollars a year; transitional frauds cost a few pounds/Euros/dollars; while the new computer crimes cost in the tens of pence/cents. In some cases, low production and distribution costs to criminals mean that direct social losses are roughly similar to criminal profits. For instance, UK consumers provided roughly $400,000 to the top counterfeit pharmaceutical programs in 2010 and perhaps as much as $1.2M per-month overall. UK-originated criminal revenue is no more than $14m a year, and global revenue, $288m. The five top software counterfeiting organisations have an annual turnover of around $22m worldwide. However, the indirect costs and defence costs are much higher for transitional and new crimes. For the former they may be roughly comparable to what the criminals earn, while for the latter they may be an order of magnitude more. As a striking example, the botnet behind a third of the spam sent in 2010 earned its owners around US$2.7m, while worldwide expenditures on spam prevention probably exceeded a billion dollars. Such defence expenditure is not necessarily irrational, but where crime is concentrated among a relatively small number of offenders who are hard to replace, it makes sense to use criminal justice mechanisms to incapacitate the offenders. For example, the number of phishing websites, of distinct attackers and of different types of malware is persistently over-reported, leading some police forces to believe that the problem is too large and diffuse for them to tackle, when in fact a small number of gangs lie behind many incidents and a police response against them could be far more effective than telling the public to fit anti-phishing toolbars or to purchase antivirus software (though this might also be desirable). This is part of a much wider problem of attributing risks to patterns of offending.

Table 1 sets out the conclusions of Anderson et al. (2012) about the costs of different forms of cyber-related crimes, *based on evidence available to us at the time* and on the organisation of those crimes and cyber-defences as they then existed. (See Riek et al., 2016 for work on indirect impacts.) As we might expect from routine activities theory, these are inherently dynamic, and even if the conclusions we came to then were valid, those costs both of crime and of prevention/responses to crime will have changed substantially in the intervening five years and projected onwards to the future. It is understandable but regrettable that cost data tend to be used well past their 'best before' date. Note also that even when attempts are unsuccessful, the immense costs to banks and other parties of protecting themselves and/or getting third parties to do so need to be factored in, and it is difficult to work out what optimal defence expenditure (or conversely, irrational expenditure) looks like in the context of almost constant attacks by private, state-tolerated and state-sponsored attackers.

Table 1: Judgement on coverage of cost categories by known estimates.

Type of cybercrime	UK estimate	Global estimate	Reference period	Criminal revenue	Direct losses	Indirect losses	Defense cost
	in million US dollars						
Cost of genuine cybercrime							
Online banking fraud							
- phishing	16	**320**	2007	x?	x?		
- malware (consumer)	4	**70**	2010	x↓	x↓		
- malware (business)	6	**300**		x↓	x↓		
- bank technology countermeasures	50	**1 000**	2010				x?
Fake antivirus	5	**97**	2008-10	x	x		
Copyright-infringing software	**1**	**22**	2010	x			
Copyright-infringing music etc	7	**150**	2011	x↓			
Patent infringing pharma	**14**	**288**	2010	x			
Stranded traveler scam	1	**10**	2011	x↓			
Fake escrow scam	10	**200**	2011	x↓			
Advance-fee fraud	**50**	1 000	2011	x↓			
Cost of transitional cybercrime							
Online payment card fraud	**210**	4 200	2010				(x)
Offline payment card fraud							
- domestic	**106**	2.100	2010				x↓
- international	**147**	2 940	2010				x↓
- bank/merchant defense costs	120	**2 400**	2010				x↓
Indirect cost of payment fraud							
- loss of confidence (consumes)	**700**	10 000	2010			x?	x
- loss of confidence (merchants)	**1 600**	20 000	2009			x?	x
PABX fraud	**185**	**4 960**	2011	x			x↓
Cost of cybercriminal infrastructure							
Expenditure on antivirus	**170**	3400	2012			x	
Cost to industry of patching	50	**1000**	2010			x?	
ISP clean-up expenditures	**2**	40	2010		x?		
Cost to users of clean-up	**500**	10 000	2012		x?		
Defense costs of firms generally	500	**10 000**	2010			x?	
Expenditures on law enforcement	**15**	400	2010			x	
Cost of traditional crimes becoming 'cyber'							
Welfare fraud	**1 900**	20 000	2011	x	(x)		
Tax fraud	**12 000**	125 000	2011	x?	(x)		
Tax filing fraud		5 200	2010	x	(x)		

Estimating costs and scaling: Figures in boldface are estimates based on data or assumption for the reference area. Unless both figures in a row are bold, the non-boldface figure has been scaled using the UK's share of world GDP unless otherwise stated in the main text. Extrapolations from UK numbers to the global scale should be interpreted with utmost caution. A threshold to enter this table is defined at $10m for the global estimate. Legend: × : included, (×) : partly covered; with qualifiers ×↑ for likely over-estimated, ×↓ for likely underestimated, and ×? for high uncertainty.

Conclusions

The articles in this volume deal 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, including the broader issues examined by Levi et al. in this volume, 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 Europol, 2016; NCA, 2016). 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. The problems of attribution to nation-state actors take us beyond the tasks addressed in this volume, but it is mentioned here because 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 polycriminal enterprises involved in the organisation of serious crimes (van Duyne and van Dijck, 2007; von Lampe, 2016; Levi, 2012).

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 we 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 (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. This includes responding to the crimes, promoting cyberfraud prevention and resilience, and more general 'reassurance policing'.

In reviewing some trends in some countries, we cannot escape the difficulties in enhancing our awareness and getting a 'truer' picture of 'what happened' in cyberfrauds – from the perspectives of victims, third parties, or law enforcement. 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". If this article and others in this volume succeed in rendering some features of cybercrimes for gain less obscure, then we will have met our objective, even if the problems of actually doing something to reduce those harms – by law enforcement or by other public and private security actors - remain quite intractable.

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T. & Savage, S. (2012). Measuring the cost of cybercrime. http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

ABS (2016). Personal Fraud, Australia, Canberra; Australian Bureau of Statistics.

BBA (2016). The Way We Bank Now: Help at Hand. London: British Bankers Association. https://www.bba.org.uk/wp-content/uploads/2016/07/TWWBN3_WEB_Help-at-Hand-2016.pdf.

Beck, U. (1992). Risk society: Towards a new modernity. Thousand Oaks: Sage.

Becker, H. (1974). Labelling theory reconsidered. Deviance and social control (pp.41-66). London: Tavistock.

Biberstein, L. Killias, M., Walser, S., Iadanza, S. and Pfammatter, A. (2016). Studie zur Kriminalität und Opfererfahrungen der Schweizer Bevölkerung: Analysen im Rahmen der schweizerischen Sicherheitsbefragung 2015. Lenzburg: Killias Research & Consulting.

Cybercrime Coordination Unit Switzerland (2015). Annual Report 2014. Bern: FedPol.

Detica, Office of Cyber Security and Information, Cabinet Office. (2011). The Cost of Cyber Crime. Guildford: Detica.

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

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 (pp. 101-124). Springer: New York.

ECB (2015). Fourth report on card fraud. Frankfurt: European Central Bank.

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

Eurostat (2015). Special Eurobarometer 423. Cyber security. Luxembourg: Eurostat.

FBI (2015). 2014 Internet Crime Report. Washington DC : FBI Internet Complaints Center.

FBI (2016). 2015 Internet Crime Report. Washington DC : FBI Internet Complaints Center.

FFA UK. (2016a). Fraud the Facts 2015. London: Financial Fraud Action UK.

FFA UK. (2016b) Year-end 2015 fraud update: Payment cards, remote banking and cheque. London: Financial Fraud Action UK.

Fitzgerald, M. (2014) 'The curious case of the fall in crime', https://www.crimeandjustice.org.uk/resources/curious-case-fall-crime

German Federal Statistics (2015). Police Crime Statistics – Federal Republic of Germany – Report 2014. Wiesbaden: BundesKriminalAmt.

Graves, J., Acquisti, A., & Christin, N. (2016). Big Data and Bad Data: On the Sensitivity of Security Policy to Imperfect Information. The University of Chicago Law Review, 83(1), 117-137.

Guardian (2013) 'Crime expert attacks 'deceptive' Home Office figures showing fall in offences', https://www.theguardian.com/uk/2013/may/05/crime-statistics-attacked-by-criminologist

Harrell, E. (2015). Victims of Identity Theft, 2014. Washington DC: Government Printing Office. *http://www.bjs.gov/content/pub/pdf/vit14.pdf*

Jardine, E. (2015). Global cyberspace is safer than you think: real trends in cybercrime. London: Chatham House. *Available at SSRN 2634590*.

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

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

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 (pp.595-622), Fifth Edition. Oxford: Oxford University Press.

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., Doig, A., Gundur. R., Wall, D., and Williams, M. (2015). The Implications of Economic Cybercrime for Policing. London: City of London Corporation. http://www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Pages/The-implications-of-economic-crime-for-policing.aspx

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

NCA (2016). NCA Strategic Cyber Industry Group Cyber Crime Assessment 2016. London: National Crime Agency.

ONS (2016a). Crime in England and Wales: Year Ending March 2016. London: Office of National Statistics.

ONS (2016b). Overview of fraud statistics: year ending Mar 2016. London: Office of National Statistics.

Paulissen, L. & Van Wilsem, J. (2015). Dat heeft iemand anders gedaan! Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland. Amsterdam: Vantilt.

Reyns, B. W. (2013). Online routines and identity theft victimization further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238.

Reyns, B.W. & Henson, B. (2016) The Thief With a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory**,** Int J Offender Ther Comp Criminol. 60: 1119-1139.

Riek, M., Bohme, R., & Moore, T. (2016). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261-273.

Scottish Government. (2014). Scottish Crime and Justice Statistics, 2013/14.

Scottish Government (2016). Scottish Crime and Justice Statistics, 2014/15.

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

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

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? Justice Quarterly, 33(5): 890-911.

Williams, M.L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. British Journal of Criminology, 56 (1): 21-48.

van Wilsem, J. (2013a). "Bought it, but never got it." Assessing risk factors for online consumer fraud victimisation. European Sociological Review, 29: 168--178.

Van Wilsem, J. (2013b) Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization. Journal of Contemporary Criminal Justice. 29: 437-453.