# Table of Contents

Assessing the trends, scale and nature of economic cybercrimes: overview and Issues.......................................................... 3

A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists....................................................... 21

Origin, growth and criminal capabilities of cyber criminal networks. An international empirical analysis........................................... 39

Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous......................................................... 55

Cyberfraud and the implications for effective risk-based responses: themes from UK research....................................................... 77
Assessing the trends, scale and nature of economic cybercrimes: overview and Issues

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

Michael Levi

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.

Introduction

When the late Ulrich Beck [1] 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?

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. [2] for a review of cost of cybercrime data; and Levi and Burrows [3] 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 [4] provided some evidence that - when combined with individual level cyber security - national cyber security strategies have some measurable effect upon victimisation, 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 [5, 6]). 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. There are many such products and articles, which are important to prevention and

---

1 See further, http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf.
2 The author is a member of the Europol iOCTA and SOCTA advisory groups.
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 conscious and unconscious 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. [7] 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 [7] 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 [8] 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\textsuperscript{3}: early iterations are therefore explicitly described as ‘experimental statistics’, [9, 10]).

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.\textsuperscript{4} 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 % 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 [9]. The accompanying note on fraud generally [10] illuminates with greater details and methodology, but I would add that though the Action Fraud reports include a variety of frauds (see [10] 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 [10] 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.

\textsuperscript{3} 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.

\textsuperscript{4} Reins [11] connects BCS 2008/9 data on identity fraud to routine activity indicators, showing higher risk for high-income households and people active online.
Almost two-thirds of fraud incidents involved initial loss of money or goods to the victim (62%), independent of any reimbursement received.

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.5

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 [12, 13]. 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 [14]. It is unwise and incorrect to demarcate heretically 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.6

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 an increase in the volume of reported identity frauds in account applications (for example, applying to open a payment card account

---

5 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.
6 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.
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 [15, 16]. 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 10 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 ([17]: 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 (6984 cases).

The Netherlands

A one-off Dutch study in 2011 [18] 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.7 A later Central Bureau of Statistics Netherlands general population study of identity fraud, consumer sales fraud and hacking by Kloosterman [21] showed that hacking was the most common form of cybercrime in 2014, affecting more than 5 % of the population, followed by acquisitions and sales fraud (3.5 %) and identity theft (less than 1 %). 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 % in 2012 to 3.3 % in 2014, outstripping the rise in the percentage who shopped online. 5.8 % of those who shopped online were victims of online shopping fraud, up from 5.3 % 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 % 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 % 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 % 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 and 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 [22].

7 see also van Wilsem’s [19, 20] 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 % in 2006 to 3.5 % in 2013 before falling to 3.1 % in 2014, and 44 % of these involved the Internet. The only acquisitive crime more common than fraud in Sweden is bicycle theft. 84 % 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/$1171). In terms of recorded fraud, compared with 2013, Computer Fraud increased by 25 % 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:

![Recorded Fraud involving the Internet in Sweden, 2006-2014](image)

Switzerland

Like other jurisdictions, Switzerland has been experiencing a rise in reported e-Crimes, rising from 6181 offences in 2010 to 10,214 in 2014, with a rising proportion of those being property offences (Cybercrime Coordination Unit [23]). 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 [24].

Australia

The ABS [25] 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 early 1930s, 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 $8421; and the median dollar loss was $560 [26, 27]. 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 % 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 1500 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 3650 individual complaints, with a total victim loss of approximately $55 million [27]. 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 [28] for a helpful discussion based largely on US data; and [29], 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**

Fifty-three percent of Canadians have been the victims of financial fraud in their lifetimes [30]. 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. Reys & Henson [31] 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 [32], 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

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of Cases</th>
<th>Financial Loss (HK$ million)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>6862</td>
<td>1828.90</td>
</tr>
<tr>
<td>2014</td>
<td>6778</td>
<td>1200.68</td>
</tr>
<tr>
<td>2013</td>
<td>5133</td>
<td>916.90</td>
</tr>
<tr>
<td>2012</td>
<td>3015</td>
<td>340.41</td>
</tr>
<tr>
<td>2011</td>
<td>2206</td>
<td>148.52</td>
</tr>
<tr>
<td>2010</td>
<td>1643</td>
<td>60.38</td>
</tr>
<tr>
<td>2009</td>
<td>1506</td>
<td>45.10</td>
</tr>
</tbody>
</table>


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/](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 [33, 34]. 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 [25] 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 et al.[35]) £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 [36]. 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. [2] 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 $1.2 M per-month overall. UK-originated criminal revenue is no more than $14 m a year, and global revenue, $288 m. The five top software counterfeiting organisations have an annual turnover of around $22 m 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$2.7 m, 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. [2] 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 [37] 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 5 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.

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 [38, 39]). As to the linkage between these and economic cybercrimes, it should be noted that there is not a
Table 1  Judgement on coverage of cost categories by known estimates

<table>
<thead>
<tr>
<th>Types of cybercrime</th>
<th>UK estimate</th>
<th>Global estimate</th>
<th>Reference period</th>
<th>Criminal revenue</th>
<th>Direct losses</th>
<th>Indirect losses</th>
<th>Defense cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost of genuine cybercrime</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online banking fraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- phishing</td>
<td>16</td>
<td>320</td>
<td>2007</td>
<td>x^2</td>
<td></td>
<td>x^2</td>
<td></td>
</tr>
<tr>
<td>- malware (consumer)</td>
<td>4</td>
<td>70</td>
<td>2010</td>
<td>x^1</td>
<td>x^1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- malware (business)</td>
<td>6</td>
<td>300</td>
<td>2010</td>
<td>x^1</td>
<td>x^1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- bank technology countermeasures</td>
<td>50</td>
<td>1000</td>
<td>2010</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fake antivirus</td>
<td>5</td>
<td>97</td>
<td>2008–10</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Copyright-infringing software</td>
<td>1</td>
<td>22</td>
<td>2010</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copyright-infringing music etc.</td>
<td>7</td>
<td>150</td>
<td>2011</td>
<td>x^1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patent infringing pharma</td>
<td>14</td>
<td>288</td>
<td>2010</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stranded traveler scam</td>
<td>1</td>
<td>10</td>
<td>2011</td>
<td>x^1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fake escrow scam</td>
<td>10</td>
<td>200</td>
<td>2011</td>
<td>x^1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advance-fee fraud</td>
<td>50</td>
<td>1000</td>
<td>2011</td>
<td>x^1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost of transitional cybercrime</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(x)</td>
</tr>
<tr>
<td>Online payment card fraud</td>
<td>210</td>
<td>4200</td>
<td>2010</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online payment card fraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- domestic</td>
<td>106</td>
<td>2100</td>
<td>2010</td>
<td></td>
<td>x^1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- international</td>
<td>147</td>
<td>2940</td>
<td>2010</td>
<td></td>
<td>x^1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- bank/merchant defense costs</td>
<td>120</td>
<td>2400</td>
<td>2010</td>
<td></td>
<td>x^1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indirect cost of payment fraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- loss of confidence (consumes)</td>
<td>700</td>
<td>10,000</td>
<td>2010</td>
<td></td>
<td>x^2</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>- loss of confidence (merchants)</td>
<td>1600</td>
<td>20,000</td>
<td>2009</td>
<td></td>
<td>x^2</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
Table 1 (continued)

<table>
<thead>
<tr>
<th>Types of cybercrime</th>
<th>UK estimate In million US dollars</th>
<th>Global estimate In million US dollars</th>
<th>Reference period</th>
<th>Criminal revenue</th>
<th>Direct losses</th>
<th>Indirect losses</th>
<th>Defense cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>PABX fraud</td>
<td>185</td>
<td>4960</td>
<td>2011</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Cost of cybercrime infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expenditure on antivirus</td>
<td>170</td>
<td>3400</td>
<td>2012</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost to industry of patching</td>
<td>50</td>
<td>1000</td>
<td>2010</td>
<td></td>
<td></td>
<td>x?</td>
<td>x?</td>
</tr>
<tr>
<td>ISP clean-up expenditure</td>
<td>2</td>
<td>40</td>
<td>2010</td>
<td></td>
<td></td>
<td>x?</td>
<td>x?</td>
</tr>
<tr>
<td>Cost to users of clean-up</td>
<td>500</td>
<td>10,000</td>
<td>2012</td>
<td></td>
<td></td>
<td>x?</td>
<td>x?</td>
</tr>
<tr>
<td>Defense costs of firms generally</td>
<td>500</td>
<td>10,000</td>
<td>2010</td>
<td></td>
<td></td>
<td>x?</td>
<td>x?</td>
</tr>
<tr>
<td>Expenditures on law enforcement</td>
<td>15</td>
<td>400</td>
<td>2010</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Cost of traditional crimes becoming ‘cyber’</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Welfare fraud</td>
<td>1900</td>
<td>20,000</td>
<td>2011</td>
<td>x</td>
<td></td>
<td></td>
<td>(x)</td>
</tr>
<tr>
<td>Tax fraud</td>
<td>12,000</td>
<td>125,000</td>
<td>2011</td>
<td>x?</td>
<td></td>
<td></td>
<td>(x)</td>
</tr>
<tr>
<td>Tax filing fraud</td>
<td>520</td>
<td></td>
<td>2010</td>
<td>x</td>
<td></td>
<td></td>
<td>(x)</td>
</tr>
</tbody>
</table>

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 $10 m for the global estimate. Legend: x: included, (x): partly covered; with qualifiers ×↑ for likely over-estimated, ×↓ for likely underestimated, and ×? for high uncertainty.
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 [40] 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 [41–43].

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 [36]. 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 [44] 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

A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists

E. Rutger Leukfeldt¹,² · Edward R. Kleemans³ · Wouter P. Stol²

Published online: 22 November 2016
© Springer Science+Business Media Dordrecht 2016

Abstract Case studies show that there are at least two types of groups involved in phishing: low-tech all-rounders and high-tech specialists. However, empirical criminological research into cybercriminal networks is scarce. This article presents a taxonomy of cybercriminal phishing networks, based on analysis of 18 Dutch police investigations into phishing and banking malware networks. There appears to be greater variety than shown by previous studies. The analyzed networks cannot easily be divided into two sharply defined categories. However, characteristics such as technology use and offender-victim interaction can be used to construct a typology with four overlapping categories: from low-tech attacks with a high degree of direct offender-victim interaction to high-tech attacks without such interaction. Furthermore, clear differences can be distinguished between networks carrying out low-tech attacks and high-tech attacks. Low-tech networks, for example, make no victims in other countries and core members and facilitators generally operate from the same country. High-tech networks, on the contrary, have more international components. Finally, networks with specialists focusing on one type of crime are present in both low-tech and high-tech networks. These specialist networks have more often a local than an international focus.

Keywords Cybercrime · Phishing · Malware · Criminal networks · Theory · Organized crime

---

¹ Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), De Boelelaan 1077a, 1081 HV, Amsterdam, The Netherlands
² Open University of the Netherlands, Valkenburgerweg 177, 6401 DL, Heerlen, The Netherlands
³ VU University Amsterdam, De Boelelaan 1105, 1081 HV, Amsterdam, The Netherlands
Introduction

‘Warning! The security of your online bank account needs to be updated. Update today or your account will be blocked. Click here to go to our secure website directly.’ Criminals use these kinds of e-mail messages to lure bank customers to phishing websites with only one goal: obtaining user credentials to clear out their bank accounts.

This article is a follow-up to the work of Soudijn and Zegers [20] and Leukfeldt [15]. These studies described phishing networks, based on police files, and showed that phishing networks can have totally different characteristics. The ‘crime script’ of the two different networks was quite similar: the formation of a criminal core group, contacting other capable criminal enablers, capturing login details from victims and transferring funds to money mule accounts. However, the origin, growth, and criminal opportunities of these networks – and thus the possibilities for crime prevention – were completely different. In the first group [20], technology played a major role: e.g. malware was used to steal user data, a forum functioned as offender convergence setting to meet new criminals, contacts between offenders were primarily online, and spam e-mails were used to recruit money mules. In the other case [15], social ties played an important role: e.g. e-mails and telephone calls were used to steal user data, other criminals were recruited through social contacts, and encounters took place on the streets of large cities.

These two case studies confirm what a priori one might expect: that cybercriminal groups are not all the same. However, empirical criminological research into cybercriminal networks is scarce (see for an overview e.g. [5, 6, 22]). Only a few case studies on a limited number of criminal groups exist. It is clear that more research into cybercriminal groups is required to map the range of possible compositions. This article takes a more comprehensive approach and analyzes all known phishing and banking malware cases in the Netherlands in the period 2004–2014. This gives more insight into the different types of criminal groups that are involved in these cybercrimes and may help to develop effective crime prevention methods.

This article uses a social opportunity structure perspective to study cybercriminal phishing and banking malware networks (see section 2 for a more detailed explanation). It elaborates upon the criminal capabilities of networks (e.g. modus operandi and the use of technology, secondary criminal activities, and international components) and the composition of networks (e.g. functions within networks). Section 3 describes data and research methods. Subsequently, the results of the study are presented regarding criminal capabilities of networks (section 4) and composition of networks (section 5). Section 6 contains a taxonomy of networks, whereas section 7 contains the main conclusions and discussion.

Social opportunity structure

The studies by Soudijn and Zegers [20] and Leukfeldt [15] show that there are at least two types of groups involved in phishing. As Leukfeldt [15] pointed out, an explanation for these differences can be found in the concept of social opportunity structure. Social opportunity structure plays a major role in organized crime networks. Social ties and networks provide access to criminal opportunities and their nature further determines the opportunity structure, which facilitates different types of crime (e.g. [9, 18, 19]). Social relationships, however, are highly clustered and therefore always limited in
certain ways (e.g. because of geographical or social barriers between countries, lack of access to different ethnic groups, or barriers between illicit networks and the licit world – see [7]: 179–180). In order to expand opportunities, it is necessary to establish relationships with ‘outsiders’ (persons outside someone’s existing social network). Therefore, access to ‘offender convergence settings’ (cf. [3, 4]) and key figures that are able to arrange these new contacts determine the growth and criminal opportunities of a given network. Studies into traditional criminal networks showed that access to these important brokers causes some offenders to remain local, whereas other offenders became international players (e.g. [9]). The local offenders commit all sorts of crimes in their own region, but they have no contacts outside their region and have no expertise others depend on. A condition for evolving into an international player is having contacts with brokers who give access to new export markets, or who have capital or expertise.

The degree of access to key figures and (digital) offender convergence settings provides an explanation for the differences between the cases described in Soudijn and Zegers [20] and Leukfeldt [15]. In fact, a parallel of the distinction between local and international offenders can be observed. The second group had no access to digital offender convergence settings and was constrained to a local social cluster. Accomplices were recruited through local social contacts and were all living in the Netherlands. All the victims were Dutch too. They also committed all kinds of other crimes to earn easy money. Conversely, the offenders of the first group met each other at a digital forum. Specific criminal services could relatively easily be acquired through the forum: victims were targeted, and accomplices were recruited in foreign countries. It also seems that the criminals were specialized in phishing attacks, as no other criminal activities were described in this case. Offenders were able to recruit new members in other countries and attack victims in multiple countries.

The social opportunity structure perspective can be used to explain differences between the nature and capabilities of cybercriminal groups described above. The two case studies show that there are differences between the criminal capabilities of cybercriminal networks and the composition of networks. In this article, we analyze 18 cybercriminal networks and test if these differences hold or need to be nuanced. The data and variables used in this article to gain insight into these elements will be described in the next section.

**Data and methods**

Eighteen Dutch criminal investigations were analyzed in order to gain insight into the composition and the criminal capabilities of criminal networks. These police files provide unique knowledge about cybercriminal networks and their members due to the use of special investigative powers such as wiretaps (telephone and internet traffic), observation, undercover policing, and house searches.

**Cybercriminal networks: a demarcation**

This study is part of the Research Program Safety and Security of Online Banking. Therefore, this study only includes networks that carry out attacks on online banking. Briefly, this means phishing attacks and malware attacks. In the literature, different definitions of phishing are used (see, for example, Lastdrager [14] for an analysis of
113 definitions). The common thread is: Phishing is the process aimed at retrieving users’ personal information by criminals who, by using digital means such as e-mail, pose as a trusted authority. User credentials can be intercepted in a more technical way, namely by using malicious software such as Trojans or spyware. This kind of malware could log keystrokes, screenshots, e-mail addresses, browsing habits, or personal information such as credit card numbers.

Case selection

In our analysis, only completed criminal investigations are used. In these cases, the public prosecutor has decided that enough evidence has been collected to prosecute the suspects successfully. This, however, does not mean that there has already been a court decision.

There is no central registration system in the Netherlands that allows for a quick overview of all criminal investigations into phishing networks. The selection of cases was, therefore, done by using the snowball method. Starting points were cybercrime and fraud teams on a national and (inter)regional level. Using existing contacts within the Dutch police and the Dutch Police Academy, team leaders and senior investigators of these teams were asked whether they knew any investigations into phishing networks. Subsequently, public prosecutors who deal with cybercrime and fraud cases were asked the same question. Furthermore, an online database in which (a limited number of) court documents are published, was used, and a media analysis was done to find news reports about phishing cases. During the file study, people involved in the criminal investigation were asked whether they knew any other phishing cases. In total, eighteen criminal investigations into phishing networks were obtained. The investigations ran between six months and three years and were carried out between 2004 and 2014.

Analytical framework

The criminal investigation files contained records of interrogations and information obtained through special investigative powers (e.g. transcripts of phone taps, internet traffic and other surveillance reports). Relevant information was systematically gathered from the investigation files using an analysis framework. The framework was based on the analytical framework used in the Dutch Organized Crime Monitor. This is a long-running research program on organized crime (see [9–13, 21]).

The analytical framework consists of a list of topics the researcher has to describe (rather than a closed questionnaire). The topics and questions of the framework include inter alia composition (hierarchy, fluid cooperation, important roles/functions, use of enablers) and criminal capabilities (modus operandi, use of technology, secondary criminal activities, working area of the network).

Interviews

The analyses of the criminal investigation were complemented by interviews with the public prosecutor, the police team leader, and senior detectives (e.g. financial or digital experts). The same analytical framework was used. The interviews were conducted because the information in the police files is aimed at providing evidence of criminal activity, meaning that other relevant information to this analysis is often lacking.
Hierarchy and secondary criminal activities, for example, are not always described. Respondents, however, were sometimes able to provide more insight into these topics.

**Criminal opportunities**

**Modus operandi**

All networks are engaged in attacks on online banking. The scripts of the crime networks have many similarities in common. The first step is to intercept login credentials from victims to gain access to their online bank accounts. However, that is not enough to transfer money from the account of victims. In order to do this, so-called ‘one-time transaction authentication codes’ are required. Obtaining these codes is, therefore, step 2. With these transaction authentication codes, transactions can be done from victim accounts to the accounts of money mules.\(^1\) Once the money has been transferred successfully, it is cashed out and, via various links, given to core members. There are some networks experimenting with other ways of cashing. These, for example, buy goods using the account of victims or buy Bitcoins. However, all networks predominantly use bogus front accounts to cash out the money.

Although the scripts of all criminal networks are roughly similar, there are some important differences. These differences concern obtaining user credentials and transaction authentication codes. The extent of ICT-use and degree of contact between the criminals and the victims differ. The high-tech capability of offenders makes it possible to limit the direct contact with the victim, but there is variation within the networks studied regarding the extent to which criminal attackers actually reduce contact with the victim. At one end of the continuum, there are networks limiting the use of ICT to a minimum and where victims issue codes to the criminals. These networks use e-mails (and sometimes phishing sites) to get user credentials. Subsequently, victims are phoned by criminals posing as bank employees in order to elicit necessary transaction authentication codes. At the other side of the continuum, there are networks using advanced malware that requires no direct contact with the victim. These networks, for example, infect websites that have outdated security. Once someone visits this website, his or her computer becomes infected with malware. This malware gives criminals access to and control over the victim’s computer and enables the attacker to adjust or change online banking sessions.

The differences between these two types of attacks relate to the extent of ICT use during the attack, as well as the degree to which criminals have direct contact with the victims. The crime scripts can, therefore, be divided into two main categories: low-tech attacks and high-tech attacks. Moreover, each category of attacks can be subdivided by the degree of interaction between offenders and victims (Fig. 1). As a result, 4 attack variants can be identified: low-tech attacks with a high degree of direct interaction between attacker and

\(^1\) In cybercrime literature, the term ‘money mule’ is often used to describe these offenders (see Choo [2]; McCombie [17]; Aston et al. [1]; [15, 20]). In our opinion, ‘money mule’ is not entirely the right term as these offenders are not used to physically move money from one place to another, but instead solely to disguise the financial trail from victims’ bank accounts leading back to the core members (see Leukfeldt et al. [16] for a more comprehensive description). As the term money mule is so widely used, we have chosen to use it in this article.
victim (10 cases), low-tech attacks with a low degree of direct interaction (5 cases), high-tech attacks with a low degree of interaction (4 cases) and high-tech attacks without interaction (1 case). Networks that are carrying out low-tech attacks sometimes use several types of attacks (both with a low degree of contact and a high degree of contact). The total number of type of attacks is, therefore, higher than the total number of networks. Below a brief description will be given for each category.

Type 1: Low-tech attacks with a high degree of victim-attacker interaction

The 10 networks executing low-tech attacks with a high degree of interaction between the criminals and victims all use phishing e-mails and websites. As a rule, victims receive an e-mail appearing to be sent by their bank. The e-mail refers to the security of online banking, and the victim is asked to take immediate action to ensure that his or her account remains secure. Sometimes the victim has to reply to the e-mail itself and sometimes via a link in the e-mail (which usually links to a ‘secure section of the website of the bank’). In both cases, offenders obtain user credentials and other relevant information. Subsequently, the victim is contacted by a member of the criminal network by telephone. The caller poses as a bank employee. During the telephone conversation, the caller refers to the phishing e-mail. Besides, the caller is able to give the victim information only the bank is supposed to know. This provides confidence that the victims are actually talking to a bank employee. During the telephone call, victims are asked to give one-time security codes, ‘to finalize the latest security updates’. Using these security codes, offenders are able to transfer money from the victim’s bank account to money mule accounts.

Type 2: Low-tech attacks with a low degree of victim-attacker interaction

Seven networks also use phishing e-mails and websites to acquire user credentials and other victim information. However, the crime script of these groups does not require a telephone call. Just like in the first attack variant, victims receive a phishing e-mail containing a link to a phishing site. This website has an additional entry field in which a telephone number has to be entered. Once the victim logs on to this phishing site, the criminals have access to the online bank account, and they consequently know the victim’s telephone number. The criminals request a new SIM card in the name of the victim. Once this has been approved by the telecom company, all communication to

![Fig. 1 Degree of technology use and contact between offender and victim](image)
the phone number of the victim goes to the criminals. Transaction authentication codes sent to the mobile phone of the user are now received by the criminals, and can be used for transactions from the victim’s bank account.

**Type 3: High-tech attacks with a low degree of victim-attacker interaction**

Networks using malware do not need to have direct interaction with victims to intercept user credentials and transaction authentication codes. The malware gives the criminal network control over the user’s computer. As soon as this has been accomplished, transfers made by the victims can be manipulated. The most important part of this attack is infecting computers of potential victims with malware. 4 networks use a method installing malware when victims click on a link in an e-mail. Network 15, for example, first hacks into several databases of companies to obtain e-mail addresses. The group also hacks a hosting company to send large amounts of e-mail via the servers of that company (in at least one case over 250,000 e-mails). The e-mail appears to originate from a major utility company in the Netherlands. The e-mail states that the recipient is in arrears and that the utility company has tried to contact the victim several times without success. It also contains a link to the invoice that has not been paid. When the recipient clicks on the link in the e-mail, the computer is infected with a Trojan. This gives the criminals control over the browser of the victim. Information the victim enters can be adjusted without the victim noticing this. Criminals alter information that the victim enters when transferring money from his or her online bank account.

**Type 4: High-tech attacks without victim-attacker interaction**

Thus, high-tech attacks also require some degree of victim-attacker interaction; if users do not click on the link in the e-mail, their computers never become infected. Network 18, however, uses an attack method in which there is no victim-attacker interaction at all. This network infected a number of websites with outdated security. When someone visits this website, his or her computer is infected with malware automatically; the user does not need to perform any actions. When the victim uses his or her online bank account to transfer money, the malware alters the highest transaction. The amount is split in two: one part goes to the original beneficiary, whereas the other part goes to the account of a money mule. The victim has to approve the transaction, as usual and enter the transaction authentication codes. The victim does not suspect anything because the total amount is not changed, and the victim does not see anything abnormal on the screen. The malware ensures that the split payment is not visible in the transaction overview of the online bank account. The only way for the victim to find out that there has been a fraudulent transaction is by logging into their online account using a computer that has not been infected with malware.

**Secondary criminal activities**

The activities of the analyzed networks are not always limited to phishing or malware attacks. In 10 cases, it is clear that core members also perform other criminal activities. It seems to be a matter of ad hoc alliances: subgroups of core members working together on specific types of crime. Sometimes core members
collaborate with people outside the core group of the analyzed network. Most criminal activities relate to financial crimes.

Six networks, for example, also carry out fraud-related activities. Five of these are low-tech networks. Two of those networks are involved in attacks on payment transactions in which technology is not used at all. These groups use postal officials to intercept newly requested debit cards and official post from the bank containing PIN numbers and login details of online bank accounts. Other groups also engage in skimming or trading stolen goods. Some low-tech groups use their money mules for other purposes than transferring money alone. In the name of these money mules, for example, tax returns are requested or multiple telephone subscriptions are registered. The phones belonging to the subscriptions are resold, and the money mules are left with the subscription fees.

Four low-tech networks are also involved in drug trafficking. This varies from setting up a cocaine line into the Netherlands to the sale of different types of pills. Furthermore, three networks are involved in burglaries, muggings, and/or trading stolen goods. One network is involved in human trafficking.

One group performing malware attacks is also engaged in credit card fraud. On forums, they buy stolen credit card information. In the Netherlands, this information is used to buy goods and to travel. Another group performing malware attacks is also involved in phishing attacks aimed at Dutch webshops (to get access to their store credit and/or credit card credentials). The core member of this network also sells goods on online auction sites without delivering these goods.

**International components**

To determine how ‘international’ a network is, we looked at the countries from which the network members operated and from where the victims originated.

In 11 cases, the core members operate from the Netherlands and only use enablers and money mules that have been recruited in the Netherlands. All these networks carry out low-tech attacks. The 7 other networks have core members (2), professional enablers (5), recruited enablers (2) or money mules (2) operating outside of the Netherlands or having been recruited outside of the Netherlands. One of these networks performs low-tech attacks. This network uses a foreign professional facilitator to develop phishing websites. The other networks with core members from outside the Netherlands are engaged in high-tech attacks.

The two networks in which the core members come from countries other than the Netherlands, use a forum to recruit professional enablers. Whether the core members themselves have become acquainted with each other through this forum is unknown.

The 4 high-tech networks use professional enablers from outside the Netherlands to purchase malware, spam services, user credentials, or money laundering services. Core members use various forums on which such criminal services are offered.

Recruited enablers from outside the Netherlands provide services to 2 networks. One facilitator sets up a ring of money mules in England; and another facilitator helps money mules from Latvia to cross the border in Ireland. Two networks use money mules from countries other than the Netherlands. One network, which operates from Eastern Europe, recruits money mules in the Netherlands and Russia. Another network recruits money mules in Latvia and arranges buses to transport them to the Netherlands.
and other countries where the network is active. Their goal is to open bank accounts, possibly with forged identity papers.

The low-tech networks are responsible for the majority of attacks on victims in the Netherlands. Twelve low-tech networks only attack customers of Dutch banks. One low-tech network also attacks people in Germany and the UK. One high-tech network only attacks customers of Dutch banks, whereas the other 4 high-tech networks also attack customers of banks in Germany, Belgium, UK, France, Swiss, and Spain.

Mapping the networks

Within all networks, there are dependency relationships and different functions. In addition to a more or less fixed group of core members, the composition of the networks changes regularly. In subgroups, core members carry out other criminal activities. Individual core members commit crimes with criminals outside the network occasionally, new enablers are recruited when crime scripts change in response to new security measures, core members are constantly recruiting new enablers, and there is a constant flow of new money mules. Despite all these changes, four positions can be recognized within all networks: core members, professional enablers, recruited enablers, and money mules.

Core members are those members of the network initiating and coordinating attacks on online banking. Without the core members, the crimes in the investigations analyzed could not be committed, and they direct other members of the network. Within the group of core members, there can also be a hierarchy. For example, one core member who directs the other core members, and subgroups of core members with a specific set of tasks. However, such a hierarchy is not a necessary part of these enterprises.

Individuals providing services to the criminal network are in the layer below the core members. These services are necessary to execute the criminal activities. Some enablers play a more important role than others for the core members. Some services are simply rarer or more sought after. Hence, also within the group enablers, a distinction can be made between professional enablers and recruited enablers. The professional enablers provide certain services to the core members, e.g. falsifying identity documents or developing malware. These enablers are qualified ‘professional’ because they offer their services to the core members on their own initiative. They, for example, offer their services on online forums which are used by cybercriminals, or they are ‘well known’ criminal enablers in the offline criminal underworld. Recruited enablers also provide services to the core members, but they are encouraged or forced by the core members to do this. They have access to information that is of interest to the core members or they are able to provide ‘simple’ services; services that core members could also perform on their own or without which the crime script could still be executed. Examples include employees of call centers of banks, postal workers and employees of telecommunication companies. Similar to professional enablers, the recruited enablers provide services to the core members. The difference between the two groups is that the recruited enablers are less important for the execution of the crime script and are more easily replaceable than the professional enablers. Recruited enablers receive a small fee for the work and are only used by one particular network.
Money mules are the bottom layer of the networks. As a rule, these people are used by the core members or by enablers to interrupt the financial trail to the core members. In all networks, amounts of money were transferred from victims’ online bank accounts to bank accounts of money mules. The money was then cashed by the money mule, a facilitator, or a core member. This makes it impossible to follow the money trail.

In all networks, we can identify core members, enablers, and money mules. However, the number of people involved in the levels of the networks differs. Network 14, for example, is a relatively small network of three core members who carry out almost all criminal acts. The core members only use a professional facilitator to obtain fake identification documents. Conversely, network 1 consists of eight core members who use at least two professional enablers and 11 recruited enablers (regarding ICT support, fake identification documents, information from banking systems, and intercepting post from banks). Naturally, we only have information about the members that came up during the criminal investigation. It is quite conceivable that there are other members of the criminal network that never attract police attention.

Core members

In 11 cases, there is information about the core members, but in the other 7 cases, the investigation stopped before core members were actually identified and could be prosecuted. This section is based on the 11 networks for which we have information about core members.

The number of core members and their tasks differs for each network. The networks consist of between 1 and 8 core members. Typical for networks with multiple core members is that during the investigation these people jointly manage the criminal activities. From that perspective, there is a group of criminals who work together for an extended period. That does not mean that the individual core members do not cooperate with other criminals outside this network. Below an outline is given of the core members of two groups with a relatively large group of core members and a relatively small group of core members. Both cases include both phishing and malware networks.

Network 1 is a phishing network consisting of 8 core members. These core members know each other from the criminal underworld in Amsterdam and work together in loosely connected subgroups. There is not one specific leader controlling the other core members. According to police respondents, this group could also represent 2 or 3 smaller criminal partnerships that employ all kinds of criminal activities and only collaborate on specific types of crime. Core members discuss how to carry out phishing attacks and how to recruit the right people, but most of the core members also have their own specific tasks. There is, for example, one core member having a contact providing fake identification documents, one core member having a contact outside the Netherlands making phishing websites, three core members being responsible for cashing the illegally obtained money, and two other core members transferring money from victims’ accounts to the accounts of money mules.

2 Money from the victims’ accounts can also be cashed in other ways. Criminals, for example, also buy goods or Bitcoins directly from the victims’ accounts. However, all networks mainly used accounts of bogus men to get the money.
Network 6 is an international network performing malware attacks. This network consists of five core members. There is one core member who directs the other core members and who has contacts with professional enablers (providing malware, spam services, and other relevant services). The other core members have specific roles, for example, getting access to online bank accounts of infected bank customers, managing the European and Russian money mules, or recruiting new money mules.

There are also networks with a limited number of core members. Network 10 performs phishing attacks and consists of a stable core group of three persons. A man and a woman who are in a romantic relationship together are responsible for all the main criminal activities. The woman calls victims, tries to obtain transaction codes, and transfers money to accounts of money mules. The man recruits money mules and directs enablers that also recruit money mules for this network. He is also responsible for cashing the money from money mules accounts. Sometimes he cashes the money himself and sometimes the person who recruited the money mules is responsible for this. In addition, a long-time friend of the main recruiter who is a major supplier of money mules is also part of the group of core members.

Network 13 carries out malware attacks and has only one core member. This person is able to gain control over bank accounts by using malware. He meets enablers from other countries on forums (e.g. to buy specific malware or e-mail addresses), whereas he directs postal employees and money mules in the Netherlands.

Professional enablers

For 15 networks, it is clear that core members use services of professional enablers, or that the network itself consists of professional service providers. In 7 of these networks, the police investigation, however, is not directed at this group of suspects and provided little insight into this group of offenders. 3 networks do not use services of professional enablers at all. The networks that do use professional enablers, use them for ICT services such as malware writing or developing phishing sites (7 networks), supplying false identity documents (6 networks), recruitment of money mules (6 networks), cashing of money (4 networks) and money laundering (1 network). Below some examples of these services are described.

The IT services used by 7 networks include the development of phishing sites, supplying large amounts of e-mail addresses and manufacturing of malware. The core members of network 13 and 15 purchase malware through a forum. One of the core members of network 15 is the technical man of this network. He is responsible for technical aspects of the crime script, such as infecting computers with malware and encrypting communication. The network uses unique malware, which has most likely been developed by the technical man himself, but this core member also uses forums to look for new criminal tools. The core member of network 13 does not make the malware he uses in attacks himself but buys malware from a forum. Furthermore, internet taps show that he frequently visits forums where criminal enablers offer all kinds of services. He places several requests on these forums, for example, to send large amounts of e-mails. He also places a call in which he asks for a programmer who can solve a specific problem with a website of a bank.

The core members of network 6 also use malware to carry out their attacks. It is unclear whether the malware was purchased or self-developed. It is, however, clear that
the core members use a forum to come into contact with people who can translate texts of phishing mails and e-mails to recruit money mules. The texts are translated from Russian into English, German, and Dutch. Furthermore, one of the core members negotiates with a member of the forum who offers spamming services that can be used to send large amounts of e-mails.

Another service for which core members use enablers is forging identity papers. Five phishing networks and one malware network used enablers for this purpose. These forged documents are used by money mules to open multiple bank accounts, to collect large sums of money in bank offices (identification is required to withdraw large amounts of money), or to send money abroad using money transfers. In none of the networks it becomes clear who these enablers actually are.

**Recruited enablers**

Networks also regularly use recruited enablers. 14 of the 18 networks use this type of enablers. Examples are money mules recruiters (N = 14), cashers who ensure the money which has been withdrawn from the accounts of money mules gets to the core members (N = 9), bank employees who, for example, provide core members with information about potential victims (N = 2), postal employees who intercept post with newly requested logins to online bank accounts (N = 2), callers who telephone victims and try to obtain transaction codes (N = 2), and an employee of a telecommunications company who is able to swap SIM cards of telephones allowing transaction codes sent to victims’ mobile phones to be redirected to the criminals (N = 1). Below some examples of money mules recruiters / cashers and bank employees will be presented.

14 networks use recruiters providing new money mules to the core members. Within 9 networks, money mules recruiters are also responsible for cashing the money. Money mules are essential to the core members because money from victim accounts is transferred to the money mules accounts. Without the bank account of money mules, the money would be transferred directly to the core members and they would be easily identified by the bank or the police. Recruiters often operate within the area in which they live and use their social network to recruit new money mules. In the case of network 8, for example, only young people in the city of The Hague are used. One of the core members of this network operates from Amsterdam. This core member is in contact with a network that is specialized in the recruitment of money mules and cashing the illegally obtained money. The group of recruiters and cashers in The Hague only recruit money mules in their own region. One of the money mules states: ‘I already said that everybody in the Netherlands is doing this. Particularly young people. You can make easy money and many want to do that. Many young people or junkies who have nothing to lose.’ This money mule was recruited on the streets of The Hague by someone he vaguely knew from his neighborhood. He came across this person ever once in a while and was offered money multiple times to lend his bank card and PIN code. Another example of recruitment within one particular area is case 10. The network of recruiters employed by network 10 only recruited money mules within a particular ethnic community in a medium-sized town in the North-West of the Netherlands. These money mules received a fee for their services, so it was not difficult for recruiters to engage new money mules. New money mules even approached recruiters on their own initiative. Interrogations provide evidence that ‘on the
street’ everybody knew that the recruiter was involved in criminal activities in which easy money could be made.

The bank employees involved in the criminal activities are all in the immediate vicinity of core members. They are approached by core members or recruiters to deliver specific services. Some bank employees reported being put under pressure; others cooperated because they got financial compensation. The bank employees provide detailed information from bank systems that is used by the core members. The bank employees work in the call centers of several large banks. In order to work there, they need a ‘Certificate of Good Conduct’. Furthermore, these employees usually have completed a relevant study (e.g. Financial Services). Through their work, these employees have access to customer data and are able to make changes in customers’ accounts. Core members use these data, for example, to cherry pick wealthy customers, to convince customers they talk with a bank employee because they can provide information that only the bank knows, and to increase cashing limits of victims’ accounts (so stolen money can be cashed more easily).

Money mules

17 networks use money mules. These people are used to break the money trail to core members. Money mules are recruited by core members themselves (4 networks), professional enablers (4 networks), and/or recruited enablers (14 networks). In most cases, money mules also offer their ‘services’ spontaneously to recruiters. This happens, for example, if a recruiter recruits long enough in one specific area. After some time, it becomes ‘common knowledge’ that easy money can be made by providing a debit card and security code. New money mules then approach recruiters or previously recruited money mules, and make clear that they also want to earn money.

Taxonomy

Section 4 and 5 provide evidence that networks have different characteristics. There are differences in the composition of networks (e.g. the number and type of enablers) and criminal capabilities (e.g. degree of technology use and interaction between offenders and victims). Additionally, international components can be recognized at different levels within the networks (at the level of core members, enablers, and victims). Finally, there are both specialists and generalists; networks carrying out one specific type of attack and networks performing a variety of criminal activities.

To provide insight into the relationship between the crime script, international components, and the degree of specialization of networks, we created a taxonomy of the networks. In Fig. 2, the 18 networks are plotted along an X-axis and Y-axis. The X-axis indicates the degree to which a network has international components. Each network has a score between 1 and 4 points. The network gets 1 point if both the core members and enablers only operate from the Netherlands, and if only victims are made in the Netherlands. If there are (also) core members or enablers involved operating from countries other than the Netherlands or if there are victims outside of the Netherlands, a network receives one extra point for each of these categories. In total, a network is able to get 4 points. The Y-axis represents the degree of technology use and the offender-
victim interaction. Again, networks can get a score between 1 and 4 points. Networks performing low-tech attacks with a high degree of offender-victim interaction get 4 points. 3 points are for networks performing low-tech attacks with a low degree of offender-victim interaction. Networks executing high-tech attacks with a low degree of offender-victim interaction receive 2 points and networks carrying out high-tech attacks without offender-victim interaction get 1 point. Finally, Fig. 2 shows whether networks consist of specialists who are engaged in one type of attack or that a network deployed all kinds of criminal activities. Specialist networks are grey in Fig. 2.

Figure 2 shows that the 18 networks cannot easily be divided into two sharply defined categories. However, there are clear differences between networks carrying out low-tech attacks and high-tech attacks. Low-tech networks, for example, make no victims in other countries and core members and enablers generally operate from the same country. The high-tech networks, on the contrary, have more international components. The 4 high-tech networks with the highest ‘international’ score consist of core members and/or enablers from different countries and get victims from several countries. The two high-tech networks with the lowest degree of international components carry out high-tech attacks in the Netherlands and operate from the Netherlands. Forums are used to recruit other suitable co-offenders in other countries (both core members or professional enablers).

Fig. 2  Taxonomy of phishing and malware networks. The X-axis indicates the degree to which a network has international components (ranging from networks with all the members of the networks and victims operating from the same country to networks with members operating from different countries and victims in different countries). The Y-axis represents the degree of technology use and the offender-victim interaction (ranging from networks performing low-tech attacks with a high degree of offender-victim interaction to networks carrying out high-tech attacks without offender-victim interaction). Finally, specialist networks carrying out one type of attack are grey. For a more extensive explanation, see section 6
Furthermore, networks with specialists focusing on one type of crime can be seen in both low-tech and high-tech networks. These specialist networks have more often a local than an international focus.

Conclusion and discussion

Conclusion

There appears to be a greater variety of networks than the empirical studies of Soudijn and Zegers [20] and Leukfeldt [15] show. Networks cannot simply be classified into high-tech networks with specialists who perform international attacks versus low-tech networks of criminal all-rounders who perform local attacks: technology use, the degree of offender-victim interaction, and international components create a more variegated set of arrangements. The most obvious differences are related to the international capabilities of low-tech networks and high-tech networks. And apparently, high-tech networks are able to carry out their attacks with fewer core members and enablers.

The crime scripts of networks have much in common. First, getting hold of credentials and one-time transaction authentication codes of victims in order to gain control over online bank accounts. Second, making transactions from victim accounts to the accounts of money mules, cashing out the transferred money, and getting the money to the core members. However, there are differences in exactly how networks carry out their crime scripts. These differences are related to obtaining user credentials and transaction authentication codes. The extent of ICT use and degree of offender-victim interaction differ. The modus operandi of the networks can, therefore, be divided into four categories: low-tech attacks with a high degree of direct offender-victim interaction, low-tech attacks with a low degree of direct interaction, high-tech attacks with a low degree of interaction and high-tech attacks without interaction.

The networks in our analysis are fluid. Although the core members of the networks form a more or less consistent group of criminals, the general composition of networks changes frequently. Subgroups of core members execute secondary criminal activities, and individual core members work together with criminals from outside the criminal network to commit all kinds of crimes.

Within all networks, four roles can be distinguished: core members, professional enablers, recruited enablers, and money mules. Core members are those members initiating and coordinating attacks on online banking. They direct and/or control the members with other roles. Enablers provide necessary services for the execution of criminal activities. A distinction can be made between professional enablers (offering their services to all kinds of criminal networks) and enablers who are recruited by core members themselves. Money mules are used by the core members or enablers to interrupt the financial trail to the core members.

Discussion

Differences between the analyzed networks mainly boil down to technology use. The higher the degree of technology use, the less interaction between offenders and victims.
Thanks to technology use, high-tech networks are able to execute successful attacks without much interaction with victims. The degree of offender-victim interaction is important because the victim has the opportunity to notice the attack during these interactions. If there is no direct interaction at all, such as in the attacks by network 18, the possibilities for users to protect themselves are very limited.

It also appears that high-tech networks more often than low-tech networks operate internationally and consist of relatively few core members and enablers. For these networks, forums play an important role as digital offender convergence settings. On forums, core members are able to search and find other suitable co-offenders and/or purchase malware to carry out attacks. Forums enable a small group of core members to have a high impact. Some of our analyzed cases show that individual core members end up at criminal forums out of curiosity. On these forums, they connect with other members, ask all sorts of questions, and experiment with offered criminal tools and services. From core members of other networks, it is unknown how they ended up at the forums they used to search for co-offenders or criminal tools. This is an important topic for further research. Questions that need to be answered include what the exact role of forums is in the origin and growth of cybercriminal networks, how core members end up on a forum for the first time, and how new criminal alliances are forged.

**Research limitations**

The analysis of criminal investigations presented in this article provides a unique view of the different roles and functions within cybercriminal networks and the criminal capabilities of these networks. The methodology, however, also has some limitations.

First of all, our analyses are based on a limited number of criminal networks in the Netherlands. We were able to track down 18 criminal investigations. Our study shows that investigations provide a good picture of the different layers and roles within cybercriminal networks and the criminal capabilities of these networks. However, because of differences in priorities, capacity, and expertise in the area of cybercrime, the same sort of analysis in other countries might provide different insights. The methodology used in our study can also be applied in other countries to supplement our analysis.

Furthermore, only criminal investigations and interviews with persons who were involved in carrying out these investigations are used. We only have information about cybercriminal networks known to and investigated (successfully) by the police. There is no knowledge about networks that remain invisible for law enforcement. For a more extensive review of methodological questions concerning the use of police investigations, see [8]. Future research should also focus on criminal networks that are able to avoid police attention and should also use other methods than file analysis.

Finally, we only analyzed cybercriminal networks carrying out phishing and malware attacks on online banking. Whether criminal networks engaged in other forms of cybercrime, such as extorting businesses with ransomware or DDoS attacks, have the same characteristics is unknown. Future research should therefore also focus on criminal networks that commit other types of cybercrime.
References

Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis

E. Rutger Leukfeldt1,2 · Edward R. Kleemans1,3 · Wouter P. Stol2

Published online: 26 November 2016
© Springer Science+Business Media Dordrecht 2016

Abstract Two recent studies which are part of the Dutch Research Program on the Safety and Security of Online Banking, present empirical material regarding the origin, growth and criminal capabilities of cybercriminal networks carrying out attacks on customers of financial institutions. This article extrapolates upon the analysis of Dutch cases and complements the existing picture by providing insight into 22 cybercriminal networks active in Germany, the United Kingdom and the United States. The analysis regarding origin and growth shows that social ties play an important role in the majority of networks. These networks usually originate and grow either by means of social contacts alone or by the combined use of social contacts and forums (to recruit specialists). Equally, however, forums play a vital role within the majority of the networks by offering a place where co-offenders can meet, recruit and trade criminal ‘services’. Moreover, those networks where origin and growth is primarily based on forums appear capable of creating more flexible forms of cooperation between key members and enablers, thereby facilitating a limited number of core members to become international players. Analysis of the capabilities of criminal networks shows that all networks are primarily targeted towards customers of financial institutions, but most networks are not restricted to one type of crime. Core members are often involved in other forms of offline and online crime. The majority of networks fall into the high-tech category of networks, mostly international, high-tech networks. These are networks with core members, enablers, and victims originating from different countries.

1 Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), De Boelelaan 1077a, 1081 Amsterdam, HV, The Netherlands
2 Open University of the Netherlands, Valkenburgerweg 177, 6401 Heerlen, DL, The Netherlands
3 VU University Amsterdam, De Boelelaan 1105, 1081 Amsterdam, HV, The Netherlands
Introduction

This article focuses on cybercriminal networks, more specifically, the origin, growth and criminal capabilities of these networks. The traditional idea is that origin and growth of criminal networks mainly operate through pre-existing social relationships; work and work-related relationships; hobbies or other activities. Cybercriminals, however, use internet forums as both a meeting place and a market place \[1–9\]. These forums use elaborate systems to show the ‘credibility’ of their members. For example, member ranking systems, ratings from earlier jobs, comments from buyers and official tests of products by administrators. Forums, therefore, provide an environment in which criminals are able to learn new tricks, plan attacks, search for co-offenders with specific knowledge or buy criminal tools. Consequently, traditional recruitment processes are changing and such change raises an interesting question: how do these developments affect the origin, growth and criminal capabilities of cybercriminal networks?

Two recent studies which are part of the Dutch Research Program on the Safety and Security of Online Banking present empirical material regarding the origin, growth and criminal capabilities of cybercriminal networks carrying out phishing and malware attacks on online banking systems in the Netherlands \[4, 5\]. Analysis of the Dutch cases shows that while social ties still play an important role in the origin and growth of the majority of networks, internet forums play a significant role in a number of networks e.g. by finding suitable co-offenders or promoting contact with enablers. Significantly, criminals with access to forums can increase criminal capabilities of their network relatively quickly. This also has implications for the criminal capabilities of networks. Different types of networks can be distinguished, ranging from locally rooted networks carrying out low-tech attacks with a high degree of direct offender-victim interaction, to international networks carrying out high-tech attacks without such interaction.

This article builds upon the recent analysis of Dutch cases and complements the existing picture of cybercriminal networks by providing insight into cybercriminal networks active in Germany, the United Kingdom (UK) and the United States (US). First, “Prior empirical research in the Netherlands” section gives a brief overview of the main findings of the analysis of the Dutch cases. “Data and methods” section contains a description of the methods used for this study. “Results” section presents the empirical results regarding origin, growth and criminal capabilities of the German, UK and US networks. Finally, “Conclusion and discussion” section contains the conclusion and discussion, which covers the results of both Dutch and the German, UK and US cases.

---

1 Phishing is the process whereby criminals use digital means such as e-mail to try to retrieve users’ personal information by posing as a trusted authority (see, for example, \[12\]). The criminal may send an e-mail that appears to originate from a trusted party such as a bank. This e-mail refers to a problem with the user’s online bank account (such as the need for a security upgrade), combined with a request for the user to take immediate action to resolve the issue (for example, by logging in using the link in the e-mail to update the account security). The aim of the attack is to intercept user credentials. These can also, however, be intercepted in a more technological way as criminals can use ‘malware’ (malicious software) such as viruses, worms, Trojan horses and spyware to obtain access to credentials or manipulate entire online banking sessions.
Prior empirical research in the Netherlands

The current article advances the work of Leukfeldt et al. [4, 5]. These articles give insight into the composition, origin and growth, and criminal capabilities of criminal networks carrying out financial cybercrimes in the Netherlands. The authors analyzed eighteen Dutch police files. These police files provided unique information about cybercriminal networks and their members largely as a result of the wide use of investigative methods such as wiretaps and IP taps, observation, undercover policing, and house searches. The files were systematically investigated using an analytical framework. This section briefly describes the main analyzed results of these 18 Dutch cases.

The structure of networks

Within all networks, there are dependency relationships and different functions. In addition to a comparatively fixed group of core members, the composition of the networks regularly changes. Subgroups of core members execute secondary criminal activities, and individual core members work together with criminals from outside the criminal network to commit a wide range of crimes. Furthermore, new enablers are recruited when crime scripts change in response to new security measures, core members are constantly recruiting new enablers, and there is a constant flow of new money mules.

Four positions can be recognized within all networks: core members, professional enablers, recruited enablers, and money mules. Core members are those members of the network initiating and coordinating attacks on online banking. Without these core members, crime in the analyzed investigations would be impossible, and they perform a directive role for other members of the network. Individuals providing services to the criminal network are in the layer below the core members. These services are necessary to execute the criminal activities. Within this group, a distinction can be made between professional enablers and recruited enablers. The first group offers services to the core members and other criminals on their own initiative (e.g. fake identity documents). The latter group provides much simpler services to the core members, and they are encouraged by the core members to do this (e.g. provide useful intelligence). Finally, money mules are the bottom layer of the networks. As a rule, these people are used by the core members or by enablers to interrupt the financial trail leading back to the core members.

Origin and growth of networks

The role of social ties in the origin and growth of cybercriminal networks certainly remains important. In the majority of networks, social ties appear to play an important role. A large number of networks in the analysis of Dutch cases have emerged and grown because core members know each other from the (offline) criminal underworld. Enablers and money mules are also often recruited through existing social networks. That does not mean, however, that forums play a marginal role. Indeed, forums play a significant role in a number of networks. For example, forums enable individuals to find suitable co-offenders in other countries. Furthermore, they provide a marketplace
for buying and selling criminal tools and services and can be used to acquire information about criminal opportunities. Various networks based on social contacts use forums to acquire specific knowledge or to buy tools. Hence, core members with access to forums are able to increase the criminal capabilities of their network relatively quickly compared to core members without access to forums.

Both social ties and forums are used to recruit new members. In this respect, four types of growth may be distinguished: (1) completely through social contacts, (2) social contacts as a base and forums to recruit specialists, (3) forums as a base and social contacts to recruit local criminals, (4) completely through forums. In the majority of networks, suitable co-offenders are still recruited through social contacts. Forums do not play an important role in all cybercriminal networks. Forums, however, do enable novel origin and network growth beyond traditional social contact. Some networks fully use these new opportunities, for example, to establish new alliances, while other networks use forums only to come into contact with criminals with specialist knowledge.

Different types of networks are involved in phishing and malware attacks. Remarkably, however, criminals without exceptional technical knowledge are largely responsible for these attacks. The core members of these networks have a long criminal career in the offline world and have manifold financial and economic crimes on their track record. From the evidence it can be deduced that the aim of these criminals is to earn easy money. They did not take a deliberate decision to commit cybercrimes as such. The analyses reveal that only one person with technical expertise is needed to carry out these cyber-attacks (who may be a core member or an enabler).

**Criminal capabilities**

All networks are engaged in attacks on online banking. Although the scripts of all criminal networks are roughly similar, there are some important differences. The differences between these two types of attacks relate to the extent of ICT use during the attack, as well as the degree to which criminals have direct contact with the victims. The crime scripts can, therefore, be divided into two main categories: low-tech attacks and high-tech attacks. Moreover, each category of attacks can be subdivided by focusing on the degree of interaction between offenders and victims. As a result, 4 attack variants can be identified: low-tech attacks with a high degree of direct interaction between attacker and victim, low-tech attacks with a low degree of direct interaction, high-tech attacks with a low degree of interaction and high-tech attacks without interaction.

To determine how ‘international’ a network is, we looked at the countries from which network members operated and from where victims originated. The low-tech networks are responsible for the majority of attacks on victims in the Netherlands. In 11 cases, the core members operate from the Netherlands and only use enablers and money mules that have been recruited in the Netherlands. The 7 other networks have core members, professional enablers, recruited enablers or money mules operating outside of the Netherlands (or having been recruited outside of the Netherlands). One of these networks performs low-tech attacks.

The criminal activities of the networks are not always limited to phishing or malware attacks. In over half of the cases, it is clear that core members also perform other
criminal activities. It seems to be a matter of ad hoc alliances: subgroups of core members working together on specific types of crime. Sometimes core members collaborate with people outside the core group of the analyzed network. Most criminal activities relate to financial crimes, but other activities like human trafficking or drug trafficking can also be distinguished.

Data and methods

This article compares characteristics of cybercriminal networks that were active in the Netherlands with cybercriminal networks in Germany, the UK, and the US. Therefore, this article uses the same analytical framework as used in the original analyses of Dutch cases.

There is a difference between the methods used to gain insight into the cybercriminal networks in the Netherlands and the countries described in this article. In the Netherlands, we had access to police files. The Dutch police files provided unique insight into cybercriminal networks and their members due to the wide-ranging use of investigative methods such as wiretaps and IP taps, observation, undercover policing, and house searches. The analyses of the Dutch criminal investigations were complemented by interviews with the Public Prosecution Service, police team leaders, and senior detectives (including financial and digital experts). This was done because the information in the police files focused on providing evidence of criminal activities, which meant that other information relevant to a scientific analysis was not necessarily included. Ties between members, for example, were not always described in detail in the files, although law enforcement actors may have had a clear picture of them. In addition to providing basic information on the number of suspects and the amounts of money involved, these interviews also revealed data on relationships within the network, binding mechanisms, and opportunity structures that were otherwise less visible.

In Germany, the UK, and the US, we did not have direct access to police files. Instead, cybercriminal networks were reconstructed solely based on interviews with case officers and/or Public Prosecutors involved in the criminal cases. Furthermore, where possible, official court documents about the cases were analyzed.

Although the method used to analyze the German, UK, and US cases did not provide us with such a detailed picture as the Dutch analyses, the current article does have added value. Firstly, the combination of methods (police files and interviews) used in the Dutch analyses showed that interviews were a good method for gaining insight into cybercriminal networks. On top of that, as mentioned above, the interviews sometimes provide better data about origin and growth and/or ties between members. Secondly, the current article provides a broader picture of cybercriminal networks. It increases current knowledge about cybercriminal networks active in or related to three other countries. Indeed, the main problem with the findings of the networks active in the Netherlands is that the study was conducted solely in the Netherlands; the same study in a different country could paint a different picture due to differences in access to information, policing priorities, and knowledge of or expertise in cybercrime.

The framework was highly dependent on the analytical framework used in the Dutch Organized Crime Monitor, a long-running research program into the nature of organized crime in the Netherlands (see e.g. Kleemans et al. [10]; Kruisbergen et al. [11]).
To make the analysis framework fit the current study, questions about the influence of digitization were added (e.g. the role of forums, the role of the internet in the recruitment of new members, etc.). Topics include the composition and structure of criminal networks, the origin and growth of networks and the use of offender convergence settings. The complete framework can be found in Appendix 1.

In total, 22 cases were analyzed: 9 in the UK, 10 in the US, and 3 in Germany. In these countries case officers were interviewed in order to gain more insight into direct ties, origin and growth, use of forums, and criminal capabilities of criminal networks. The interviews with Dutch case officers and Public Prosecutors showed that these in-depth interviews provide enough information to get a complete picture of the criminal network investigated. Court documents and open source information (e.g. news articles about the case) were used to complement the information provided by the respondents. The 22 cases analyzed covered the period 2003–2014. The interviews about these cases were conducted between March 2014 and November 2015.

Contacts with law enforcement agencies in the different countries were made using existing contacts within the Dutch police (especially the Dutch High Tech Crime Unit) and the Dutch Police Academy. Similar to the selection of Dutch investigations, it was also difficult in these countries to get an overview of completed criminal investigations into cybercriminal networks. Therefore, we used the snowball method. First contact was made with cybercrime teams at the national level: in the UK the NCA (National Crime Agency), in the US the USSS (United States Secret Service) and FBI (Federal Bureau of Investigation), and in Germany the BKA (Bundeskriminalamt). After a first meeting with the team leader, follow-up appointments were scheduled with case officers who had been involved in relevant criminal investigations. With the NCA an agreement was drafted concerning data collection and the use of data.

In the next part of the article, we describe the results of our analyses. Throughout the text, we refer to specific criminal networks. Networks with number 1 to 9 inclusive are part of UK investigations, networks 10 to 19 are part of US investigations, and networks 20 to 22 originate from German investigations.

Results

Origin and growth

The Dutch cases showed four types of growth: (1) completely through social contacts (2) social contacts as a base and forums to recruit specialists (3) forums as a base and social contacts to recruit local criminals and (4) completely through forums. The UK, US and German networks can also be broken down into these four categories. Regarding 21 networks, we have information about the origin and growth processes.

Origin and growth: social ties

Social ties play an important role in the origin and growth of 16 networks. In eight of these networks, origin and growth is entirely based on social ties. Within eight other networks, social ties form the base, while forums are used for the recruitment of enablers. In these networks, core members and sometimes the most important enablers
know each other because they grew up in the same community, have committed offline crimes together or have been in the same prison.

Network 1, for example, is composed of members originating from the Nigerian immigrant community in London. All three core members participated in computer science related degrees at universities. Two of the core members met each other at university during their studies. The core members posted fake job advertisements on online job sites. Clicking on links in the adverts resulted in malware infection. The malware was purchased through a forum. With the help of employees within banks recruited from within the same community, transfer limits of victims’ accounts were increased. The core members themselves then recruited money mules within their community. Often, according to respondents, they looked for young and gullible women.

Network 6 and 7 consist of core members who know each other from the underworld of respectively Vietnam and London. Both networks consist of a stable group of core members who have been working together for some time and using enablers — who, for example, provide money laundering services or networks of money mules — they know from the criminal underworld.

Another example is network 11. The two leading core members of this network, establishing and controlling a major international platform on which (cyber) criminals could make payments to each other anonymously, grew up in the same neighborhood.

The two core members of network 13 went to the same university. These core members hack into databases from large companies to steal large quantities of debit card and credit card information. They sell these data in bulk to five wholesalers they all know from the ‘offline world’.

Origin and growth: forums

Five networks mainly use forums for origin and growth. Within four of those networks, the core members know each other through forums and recruit enablers to help them carry out specific parts of the crime script. One network (network 15) has only one core member. This core member used forums to find enablers and sell stolen personal data.

Network 3 is a network using homemade malware to steal user credentials from infected computers, and manipulating internet banking sessions. Two of the four core members have known each other online for a long time. They met each other in a chat group on a forum where advanced programmers discuss coding. They have never met in real life according to the respondent. Through other forums they contacted two other coders who help to programme specific parts of the malware.

Network 20 has the same kind of history. Two of the five core members of this network have known each other for years because they are active in online communities and many are active on chat channels about programming, hacking, and fraud. The other three core members joined the group later, but according to the respondent, all have prominent reputations in the online community and have committed various digital crimes (for example, DDoS attacks, ripping movies, and fraud on online auction sites). The network uses an exchanger (a person converting digital currency into real money) on a regular basis. This exchanger advertises his services on several forums.

In conclusion, social ties play an important role in origin and growth processes of 16 cybercriminal networks, while the origin and growth of five networks are primarily
based on forums. It is striking that within these cases, examples of prolonged, repeated interaction through online communities can be distinguished, in addition to a more ad hoc search for suitable co-offenders and enablers.

**Roles and functions**

Regarding all 22 networks, we have specific information about roles and functions. Three networks solely consist of one group of core members. The core members of these networks are able to perform all the steps in the crime script. In all three cases, these networks are specialized in a particular service and also commit fraud. Network 3, for example, develops malware and sells this malware on forums. The group also uses this malware to harvest credentials of customers of financial institutions and markets these credentials via a forum. Network 16 is engaged in the purchase and sale of customer data from financial institutions and provides services to change virtual money into real money and vice versa. Finally, network 18 manages a botnet which can be rented by third parties, for example, to send spam or carry out DDoS attacks. This network also steals user credentials from the computers that are part of the botnet and manipulates Internet banking sessions.

Core members of seven networks use enablers and core members of two other networks to directly manage and control money mules. Core members use enablers for different services: recruitment and/or management of money mules (8), money laundering (3), exchanging digital currency (3), digital tools (3), customer data of financial institutions (2), hacking (2), bank employees being able to alter account settings (2), postal workers being able to intercept post from financial institutions (2), telephone callers (1), and identity forgers (1).

Similar to all Dutch networks, ten of the networks consist of a group of core members, (professional or recruited) enablers, and money mules. The core members are the group of criminals who initiate the criminal activity and without whom the particular offense from the analyzed investigation would not have been committed. Enablers provide specific criminal services. Based on the interviews, it is difficult to distinguish between professional and recruited enablers. Money mules are used to conceal the money trail to the core members (for more information, see [5, 13]).

**Structure**

As in the Dutch cases, there are dependency relationships and different functions within most networks. In 20 networks, we have specific information about their structure: 16 have a relatively fixed group of core members; and 4 networks consist of core members who co-operate together on an ad hoc basis alongside other criminals.

The networks consisting of subgroups of core members working on an ad hoc basis with each other use forums to find suitable co-offenders (both core members and enablers). These networks are all part of category 3 or 4 types of growth: forums as a base and social contacts to recruit local criminals; and growth completely through forums, respectively. Network 12, for example, is a fluid network of cooperating individual offenders using a forum to find the best criminals to carry out a phishing attack. At the time of the investigation, the network consisted of 10 people. One core member is the coordinator who plans and manages the involvement of others and is in...
charge of, for example, the distribution of the money. The ‘others’ are enablers who provide e-mail addresses, create phishing websites, translate texts, put data on credit cards or manage networks of money mules etc. The harvested credentials of banking customers are then partially abused by the core members themselves and partly sold via a forum. In addition to this, core members also use a forum to buy credit card information stolen by other networks.

Network 20 consists of a group of five core members. All core members have already committed various digital crimes and have “won their spurs” in the online hacking community. Two core members have known each other for years and met online through a chatroom on programming. For this specific attack, these two core members enlisted the help of three others because the latter had the capacity to adjust specific parts of malware owned by the two core members.

It would appear that social ties are an important factor for a stable group of core members. Networks with a solid group of core members are usually networks of category 1 and 2: growth completely through social contacts; or social contacts as a base and forums to recruit specialists. Eight networks have members that have been active in the criminal environment and committed miscellaneous offline crime. They originate from the same communities within big cities and/or know each other from jail or earlier criminal jobs. In a number of networks, there is also a link with traditional organized crime. Network 7, for example, consists of core members who have known each other for many years from the London underworld and have strong ties with traditional organized crime in London. For their crime script, these core members need enablers providing hacking services, recruited through existing criminal contacts from a different country. Network 9 and 10 originate from a traditional criminal network that committed all sorts of offline crimes. According to respondents, they are probably also associated with traditional organized crime in Russia. Finally, network 22, a locally operating network in Berlin, has close links with a criminal motorcycle club. The motorcycle club is responsible for managing money mules.

There are also networks with a stable group of core members in which real-world social ties do not play a role. Within these networks, online contacts form the basis. Network 15, for example, consisted originally of one core member stealing user credentials on his own and selling these on his own website. This core member recruited three others online who were running a franchise of the websites established by the original core member. In addition, the four core members of network 3 originally met on a forum, but have been working together for a long time. They have developed malware allowing them to capture user information and manipulate internet banking sessions. They use a forum to sell the malware they have developed.

**Criminal capabilities**

In order to gain more insight into the criminal capabilities of the networks, we looked at the crime scripts, international components, and the degree of specialization of networks.

All networks are engaged in attacks on customers of financial institutions. In the Dutch cases, the attacks boiled down to phishing and malware attacks. This is also true for most of the international cases. Three networks carry out phishing attacks and 10 networks carry out malware attacks (of which two networks do not attack customers
directly, but infect bank computers). Four networks hack into databases containing credit and debit card information, or hire hackers to do so. Four networks buy credit and debit card information on forums. One network operates solely as an enabler for a specific part of the crime script for other networks and does not carry out attacks itself.

The crime scripts can be divided into two categories: networks attacking customers of banks (using malware and phishing attacks) and networks attacking companies controlling financial data of customers i.e. hacking into databases containing credit card and debit card information or hacking directly into the bank systems.

There is a difference between the attacks in the degree of offender-victim interaction. This means there is a difference in user protection against attacks. Phishing attacks require a high degree of offender-victim interaction. Firstly, the victim has to respond to an email and log on to a phishing website to provide login credentials. Secondly, the criminals have to acquire one time security codes to transfer money to money mule accounts. This requires criminals to telephone victims, pose as a bank employee, and convince victims to hand over these codes which can only be used within a short period of time. Malware attacks require a much lower degree of offender-victim interaction. Criminals use emails to lure victims to infected websites, or add infected attachments to emails. Once the victim surfs to the infected website or opens the infected attachment, the computer is infected and is under the control of the criminals. The crime script with the lowest degree of offender-victim interaction is hacking into companies controlling financial data of customers. In those cases, customers of financial institutions are not directly involved in the attack.

Most of the criminal networks analyzed are not dedicated to just one type of crime. Only seven of the 22 networks could be characterized as specialized. The core members of these networks commit only one type of crime whereas the core members of 15 networks are also involved in other types of crime. Nine of these networks also commit offline crime, such as drug trafficking, arranging fake marriages, fraud, robbery, and identity forgery. Core members of five networks are engaged in other forms of cybercrime e.g. renting a botnet for spamming or DDoS attacks, phishing or credit card fraud (in these cases not as the main criminal activity, but as a secondary activity), and mining bitcoins using computers which are part of a botnet.

To show the relationship between the crime scripts, international components, and the degree of specialization of networks, we created a taxonomy of the networks. In Fig. 1, 21 networks are plotted along an X-axis and Y-axis. The X-axis indicates the degree to which a network has international components. To determine how ‘international’ a network is, we looked at the countries from which the network members operate and from where the victims originate. The network receives 1 point if both core members and enablers operate from the country from which the police investigation originates and if victims in that country are targeted. If
there are (also) core members or enablers involved operating from different countries or victims in different countries, a network receives one extra point for each of these categories. In total, a maximum of 4 points is attributable. The networks are plotted in Fig. 1. Finally, Fig. 1 shows whether a network consists of specialists who are engaged in a singular type of attack (shaded) or one that deploys all kinds of criminal activities.

Figure 1 shows the majority of analyzed networks fall into the category of high-tech networks, mostly international high-tech networks. These are networks in which core members, enablers, and victims originate from different countries. None of the networks fall into the category of local low-tech networks. This is a clear difference from the Dutch cases, of which over half of the networks fall into that category (this difference will be discussed below). Finally, in all three categories, there are specialized and non-specialized networks.

**Conclusion and discussion**

The aim of this study was to complement the current picture of the origin, growth and criminal capabilities of cybercriminal networks. Using the same analytical framework as Leukfeldt et al. [4, 5], we analyzed 22 criminal investigations into cybercriminal networks operating in the UK, US, and Germany. Although the current analysis provides valuable insight into the origin, growth, and criminal capabilities of cybercriminal networks, it also has several limitations (for a more detailed overview of pros and cons of the use of police files see, for example, [14]).
Research limitations

Firstly, there may be a selection effect. The existing contacts with police, especially within the high-tech crime unit, might have led to criminal investigations of high-tech networks. By using the snowball method within a limited time frame, it is possible that we were directed to ‘interesting’ and ‘spectacular’ cases. This may explain differences with the Dutch cases; there was more time available for the selection of Dutch cases, resulting in identifying all investigations into cybercriminal networks and thereby examining a cross-section of cases handled by Dutch police. Rationing of cases for prosecution may play a role as well, as the international cases were selected through national agencies (such as, e.g., the NCA in the UK). This may explain why category 1 networks were absent in the international sample, whereas for the Dutch cases, this was an important category. The importance of this article, however, clearly does not lie in ‘quantifying’ statements. Its aim is to provide more insight into the different types of origin and growth processes and the related criminal capabilities of cybercriminal networks. The results can serve as a starting point for future studies into the functioning of cybercriminal networks.

Furthermore, this analysis is limited to criminal networks engaged in attacks on (customers of) financial institutions (i.e. phishing or malware attacks and hacking into credit and debit card databases). Therefore, it is unknown whether these findings apply to other types of networks, for example, networks of cyber extortionists or distributors of child pornography.

Finally, this analysis only covers cybercriminal networks which are part of a criminal investigation. Therefore, there is only insight into those networks which are under investigation by the police. Networks that remain under the radar of police are not included in the analysis. Future research should also focus on networks not known to the police. This could, for example, be done in cooperation with commercial security companies monitoring parts of the Internet (including digital meeting places) for their clients.

Conclusions

The analysis of the UK, US, and German networks confirm the picture of four different types of growth that were derived from analysis of the Dutch cases: (1) completely through social contacts, (2) social contacts as a base and forums to recruit specialists, (3) forums as a base and social contacts to recruit local criminals, (4) completely through forums.

The picture of real-world social ties playing an important role in the majority of networks can be confirmed: this is true for 16 of the 21 networks where we have information about origin and growth. For eight networks, origin and growth were entirely based on social ties and in 8 other networks social ties are the base, whereas forums are used for the recruitment of enablers. For five networks, origin and growth are primarily through forums. Using these digital meeting places, core members meet, recruit enablers and/or sell their criminal services or stolen personal data. It is striking in these cases to find examples of prolonged, repeated interaction through online communities, in addition to the more ad hoc searching and finding of suitable co-offenders and enablers on forums.
Analysis further shows that forums play an important role for the majority of the cybercrime networks. Forums play a role in 18 of the 22 networks and are used by the networks for different purposes: recruiting enablers (4), purchasing tools and services (9) and selling tools and services (9). The four networks that do not use forums at all originate and grow from social ties alone.

In addition, forums appear to provide a more fluid form of cooperation of key members and enablers. A limited number of core members (or even a loner) can thus become international players. Alongside access to a forum it would appear that only one good technician who makes malware, manages a botnet, or hacks into databases is required.

In contrast to the Dutch cases, the structure of the other networks seems to be more diverse, sometimes lacking core members, enablers, and money mules. Core members sometimes perform all aspects of the crime script themselves but even here forums play an important role. On the one hand, this is because there are specialists creating malware or stealing large quantities of financial data by hacking into databases. These groups sell their data to others who resell it on to criminal groups or loners. It is unnecessary, therefore, for these groups to have an entire network of enablers and money mules. On the other hand, there are groups which do not steal information from individuals themselves, but simply purchase the information on a forum or through reliable partners. These groups are dependent on others, but need only a limited number of enablers to carry out their crime scripts.

All networks engaged in attacks on customers of financial institutions. The crime scripts can be divided into two categories: networks using malware and phishing attacks to attack customers of banks, and networks attacking companies controlling financial data of customers. These different crime scripts relate to a different degree of offender-victim interaction and thus a difference in the opportunity for users to protect themselves against attacks. Phishing attacks require a high degree of offender-victim interaction, malware attacks require a much lower degree of offender-victim interaction, whereas hacking into companies controlling financial data of customers, requires no offender-victim interaction at all.

It is also striking that, compared to the Dutch cases, the networks in the US, UK, and Germany more often seem to carry out high-tech attacks. Only 3 of the 22 networks carry out low-tech phishing attacks. The networks are also much more international in nature than the Dutch networks analyzed. Core members, enablers, or victims are from different countries. This finding might be caused by the aforementioned selection effect: the existing contacts with police might have led to more high-tech cases or ‘interesting’ and ‘spectacular’ cases.

Discussion

Real world social ties continue to be important in the origin and growth processes of cybercriminal networks. Forums, however, seem to be crucial for a change in the origin and growth of networks, and thereby criminal possibilities. For the majority of the cybercriminal networks, forums play a role in one way or another: as a ‘social’ meeting place, for buying services, or as a platform for selling stolen goods.

The networks whose origin and growth mainly take place on forums form a special group: they are more fluid than the other networks and a network with a relatively small group of core members is capable of becoming an international player. Indeed, forums
ensure that traditional limitations of social ties - especially contacts outside the initial social cluster and recruitment processes dependent upon trust-building - can be overcome. In other words, forums seem to make it possible to quickly make new contacts and expand criminal possibilities.

The members of criminal organizations in which forums play a significant role, would often appear to have been from an early age interested in information technology and often frequent chat groups related to programming. Consequently, it may be interesting to study the young people who are exploring the possibilities of programming or other applications of new technology and, in particular, processes which facilitate or prevent crossing the line to becoming involved in cybercriminal activities.

Notably, it is striking that the networks whose core members met online, are not always fluid in nature. Within these networks we can find examples of relatively stable groups of core members and enablers. Thus, not only real-world social ties enable a stable network, but on some occasions, also virtual-world social ties can operate in a similar way.

An entirely different question is the relative importance of what is going on at forums (see, e.g., [2]). Are forums not simply filled with what is referred to as ‘low-hanging fruit’? It is, after all, remarkable that the analyzed networks responsible for stealing millions of credit and debit card credentials, or infecting millions of computers with malware, do not sell this data directly on forums. Instead, they sell their business or services through several layers of intermediaries. Indeed, the source of evil is not on the forum. More research into the role of forums within cybercriminal networks should provide more insight into this challenging issue.

Appendix 1: Analytical framework

Direct ties

- Describe the composition of the criminal network: how are the suspects related, their role and/or function within the network (subgroups, core functions, facilitators, periphery).
- Describe the structure of the criminal network (standalone unit, fluid cooperation based on a specific goal).
- Is there a hierarchy and / or mutual dependency?

Origin and growth

- How, when and where did the criminal cooperation start?
- Do the suspects have a common background? (Family, neighborhood, friends, occupation, place of origin, etc.). If not, in what way are the suspects related and how did the cooperation start?
- What kept the members of the criminal network together? (e.g. social ties, economic advantages, fear, etc.).
- Describe the period/duration of the activities.
- Describe changes within the composition of the criminal network.
- How are new members being recruited?
Offender convergence settings

– Describe the (digital) offender convergence setting used by the criminals.

Modus operandi

– Describe the main criminal activities of the network (describe the MO in detail in the next section)

– Describe secondary criminal activities of the network and individual offenders.

– What is the working area of the network (region, country, interaction, certain banks).

– Who are the suitable targets for this network? (which type of people are attacked).

References

Do police crackdowns disrupt drug cryptomarkets?
A longitudinal analysis of the effects of Operation Onymous

D. Décary-Hétu1 · L. Giommoni2

Published online: 29 October 2016 © Springer Science+Business Media Dordrecht 2016

Abstract In recent years, there has been a proliferation of online illicit markets where participants can purchase and sell a wide range of goods and services such as drugs, hacking services, and stolen financial information. Second-generation markets, known as cryptomarkets, provide a pseudo-anonymous platform from which to operate and have attracted the attention of researchers, regulators, and law enforcement. This paper focuses on the impact of police crackdowns on cryptomarkets, and more particularly on the impact of Operation Onymous, a large-scale police operation in November 2014 that targeted many cryptomarkets. Our results demonstrate that cryptomarket participants adapt to police operations and that the impact of Operation Onymous was limited in time and scope. Of particular interest is the finding that prices did not increase following Operation Onymous, even though many dealers retired shortly after it occurred.

Keywords Cryptomarket · Police crackdown · Displacement · Illicit drug market

Introduction

While initially conceived as a tool to share information, the Internet has now become an important platform on which illicit goods and services can be bought and sold. This thriving underground economy is fuelled by a dramatic growth in the number of

∥ D. Décary-Hétu
david.decary-hetu@umontreal.ca

L. Giommoni
GiommoniL@cardiff.ac.uk

1 École de criminologie, Université de Montréal, Pavillon Lionel-Groulx C.P. 6128, succ.
Centre-ville, Montréal, QC H3C 3J7, Canada
2 School of Social Sciences, Cardiff University, Cardiff, Wales, UK
individuals who participate in online illicit markets and an ever-increasing range of
goods and services that are made available [1, 2].

These markets traditionally focused on computer hacking, financial fraud and
intellectual property fraud. Starting in 2011 however, a new breed of online illicit
markets appeared, focusing on a whole new line of products: illicit drugs [3].

The European Monitoring Centre for Drugs and Drug Addiction points out that “the
growth of online and virtual drug markets poses major challenges to law enforcement
and drug control policies.” ([4]: 34). Indeed, online illicit markets, through the adoption
of mitigating technologies, make it possible to sell any substance across the world. This
new distribution channel, if adopted widely by drug dealers and drug users, holds the
potential to disrupt the distribution and sales of illicit drugs, and consequently, to
disrupt the ability of law enforcement to regulate these illicit markets. For now, little
has changed in law enforcement’s approach which has focused on arresting and
prosecuting online drug dealers, seizing their money, their drugs and the online markets
they operate from [5, 6]. This strategy has had only limited success according to
international agencies [4, 7–9], who have called for a deeper understanding of
cryptomarkets, the name given to the new breed of online illicit markets: “EU law
enforcement, Europol included, has not fully conceptualised how to integrate this cyber
dimension into all relevant aspects of police work, let alone devise a strategy and
implementation plan to make this happen” ([8]: 71). Some researchers have gone a step
further and criticized the law enforcement strategies, arguing that they foster competi-
tion and innovation among online offenders and inadvertently provide free publicity to
cryptomarkets [10, 11]. Law enforcement operations displace participants to alternative
online drug markets but do not limit their activities [10, 12].

This paper will build on these research findings and provide a deeper understanding
into how cryptomarkets react to law enforcement interdiction. The main objective of
this paper is to describe and explain the impact of police crackdowns on cryptomarkets.
To do so, this paper will center on a case study of the largest law enforcement
intervention against cryptomarkets, Operation Onymous. The first section of the paper
presents the literature on the enforcement of physical illicit drug markets and more
particularly the impact of police crackdowns. The following section describes how
cryptomarkets operate and have evolved. After introducing our data and methods, we
then describe the state of cryptomarkets before and after Operation Onymous. Our
results show that the operation did impact cryptomarkets in general but that this impact
was limited to less than 2 months; some participants also displaced their activities
following the operation. The conclusion present prospects for future research.

The enforcement of traditional illicit drug markets

The strategies to regulate illicit drug markets can target either the supply or the demand
for illicit drugs. Demand control programs attempt to cut drug consumption by
reducing the number of users and/or the quantity of drugs they consume [13, 14].
Opioid substitution therapy and school-based drug education programs are typical
examples of interventions aimed at reducing the demand for illicit drugs. Supply
control programs affect drug consumption by targeting drug prices and availability
[15]. The risks and prices model of Reuter and Kleiman [15] assumes that compensation
for non-monetary costs (risk of law enforcement and violence) is the main factor driving up the price of illicit drugs [16]. Law enforcement thus works like a tax, imposing additional costs on suppliers, who then pass them on to drug users [15]. Users, in turn, adjust their consumption habits according to drug prices. The main difference, then, between demand side and supply side actions is that demand programs aim to affect drug use directly while supply programs aim to do so indirectly. While supply and demand programs can coexist, supply side programs have always received more attention and funding [17, 18], even in countries with a lenient approach to drug use, such as the Netherlands [19].

Supply side actions can target many links in the supply chain through a wide range of programs (see [20]). Of these, supply side enforcement efforts aimed at disrupting specific marketplaces (crackdowns) are the most popular [21]. Crackdowns can be generally defined as an intensive police operation characterized by increased severity or certainty of sanction and by a public relations campaign to advertise the operation [22]. Despite their popularity, there is limited evidence to support the effectiveness of police crackdowns in reducing the supply and/or demand of illicit drugs ([22–28]). Indeed, most studies have found that police crackdowns have no or little impact on the number of drug users or suppliers ([25, 28]), drug prices [23, 25, 27, 28], or the number of users entering treatment centres [25, 27, 28]. Mazerolle et al. [26] point out that classic police operations are less likely to reduce street-level drug market problems than alternative approaches (community-wide policing, problem-oriented policing, hotspots policing).

While little evidence supports the use of police crackdowns to reduce the number of drug market participants and sales over the long term, there have been indications that crackdowns can have a time-limited impact on drug markets [25]. This impact is, however, offset by the adaptation of market participants through displacement techniques [24, 25, 28].

Tactical displacement, the replacement of a crime commission script by another, is the most common form of adaptation to enforcement efforts against illicit drug markets. Police interventions may lead to a shift from “open” to “closed” drug markets with dealers that may adopt technological solutions such as cell phones and messaging applications to contact their suppliers and customers covertly and evade surveillance [24, 25, 29–31].

Open markets are generally specific locations where drug users go to buy illicit drugs and are characterized by higher risk (both of enforcement and violence) since buyers deal with the dealers that are available at that moment and at that place rather a dealer they know. Closed markets are not tied to specific locations and work more like a network that only trusted participants can join. There is ample evidence that demonstrates that drug market participants have turned open markets into closed ones after police crackdowns in order to reduce the risks of enforcement [24, 32, 33].

Geographical displacement is another common form of adaptation to police operations. Several studies have shown that police crackdowns are unable to reduce the number of transactions but may lead to a change in the physical location where dealers and users meet [23, 24, 28, 34, 35]. For instance, Wood et al. [28] show that a large scale police crackdown in Vancouver had no impact on the price of illicit drugs, the frequency of use, or the level of enrolment in treatment programs. Instead, their findings suggest that this large police operation merely displaced drug use from the
area of the crackdown into adjacent areas of the city. Such displacement was however not seen in other controlled experiments [36].

**Cryptomarkets and law enforcement**

While displacement in traditional drug markets is well understood, there are no best practices on how to enforce online illicit markets, and even less so for cryptomarkets. This is due in part to the scarcity of enforcement operations that have targeted cryptomarkets and to the recent emergence of these online illicit markets. It is likely that the particular nature of cryptomarkets will change the size and scope of the impact of enforcement. To understand how and why this is the case, we will now describe the characteristics of cryptomarkets and their evolution over time.

Cryptomarkets are websites that allow participants to buy and sell goods and services while providing some level of anonymity [3]. They are sometimes used to sell hacking services, fake ID cards and stolen financial information. Most of their activities however focus on the sale of licit drugs sold illicitly (prescription drugs) and the sale of illicit drugs (cannabis, stimulants, novel psychoactive substances). The cryptomarkets’ innovation originates not in the development of a new stealth technology but rather from the combination of many technologies that, when combined, provide an enhanced level of anonymity to participants. These technologies protect the identity of the participants by routing all of their traffic through the Onion Router (Tor) network [37], making it very difficult to find the participants’ IP address as well as the IP address of the servers hosting the cryptomarkets. The anonymity of the participants is further enhanced by the use of bitcoins [38] as the method of payment for purchases. Bitcoin is a virtual currency that can be exchanged online instantly and without having to identify either end of a transaction.

The first cryptomarket was SILK ROAD (SR1), which rose to fame through a 2011 news stories by Gawker Media that described it as “the underground website where you can buy any drug imaginable” [39]. Figure 1 shows the main page of SR1, which resembles licit merchant websites such as eBay and Amazon. The FBI estimated that total sales on SR1 from February 2011 to October 2013 were in the range of $200 million USD [40]. This translates to about $80 million USD on average per year, a figure that is close to the one provided by academic researchers [1]. This marks a sharp increase from the 2012 estimate of $14.4 million USD by Christin [41] who used a very similar methodology to that used by Aldridge and Décary-Hétu [1] but represents much less than 1 % of the overall illicit drug trade.

So far, two major police operations have targeted cryptomarkets. The first, on October 2, 2013, led to the shutdown of SR1 by US law enforcement, the seizure of over $33 million USD in bitcoins, and the arrest of its founder and administrator [42]. SR1’s participants quickly moved to other cryptomarkets, including AGORA, CLOUD-NINE, EVOLUTION, HYDRA, SHEEP, and SILK ROAD 2 (SR2).1 A number of these cryptomarkets were active for only a short time as they were taken down during a second police operation, “Operation Onymous,” launched on November 5, 2014. Operation Onymous was a combined effort by law enforcement agencies from 16

---

1 SR2 was somewhat affiliated with SR1 as its main administrators had been moderators on SR1.
European countries and the US and led to the arrest of 17 people, including the administrator of SR2. It also led to the seizure of over $1.3 million USD in bitcoins, cash, precious metals, and drugs. At the time of Operation Onymous, the cryptomarkets with the most listings – the online name for a product page and a proxy for the size and relevance of cryptomarkets - were, in order, AGORA, SR2, EVOLUTION, ANDROMEDA, BLUESKY, CLOUD-NINE, and HYDRA [10].

The adaptation of cryptomarket participants to police operations

The launch of Operation Onymous confirmed the law enforcement’s ability to target cryptomarkets and raised questions about the relative impunity and anonymity of participants. It also proved that shutting down SR1 was not a fortuitous event but possibly the first of many operations targeting cryptomarkets. Past research [10, 11] concludes that the fear created by the police operation against SR1 was not sufficient to deter participants who were able to adapt through displacement.

The first displacement technique used by participants was to virtually move to new cryptomarkets. In the aftermath of SR1’s shutdown, many participants moved to BLACK MARKET RELOADED (BMR) and SHEEP [11]. In the 6 weeks following the shutdown of SR, BMR saw a twofold increase in the number of dealers; SHEEP’s number of dealers was multiplied by more than four. Buxton and Bingham [10] describe a similar virtual geographical displacement of participants following Operation Onymous, with activity on AGORA and EVOLUTION increasing in the subsequent weeks. Soska and Christin [12] provided the most comprehensive study of the longitudinal evolution of the cryptomarket’s ecosystem, showing its resilience to
both scams and shutting downs. The authors show that shortly after the take down of SR, a vast part of the sales were absorbed by BMR, indicating the shift of sellers and buyers to the new cryptomarket. By contrast, they find that Operation Onymous significantly affected sales in the cryptomarket system, although sales in Evolution and Agora started growing quickly after a few weeks from the police intervention.

Buxton and Bingham [10] observe also that, following these two main police operations, participants adopted more secure communication techniques, using out-of-band communication channels and point-to-point encryption to exchange messages. Cryptomarkets implemented more secure authentication methods, such as two-factor authentication. Participants also discussed about the possibility of moving cryptomarkets to a decentralized architecture which would limit the possibility of market take downs (see [43] for an example).

Modeling the impact of law enforcement on cryptomarkets

The limited literature on the impact of law enforcement on cryptomarkets provides some insights on how cryptomarkets react to law enforcement interventions. However, as Soska and Christin outline “[t]he effect of law enforcement take-downs […] is mixed at best” (2015: 41) though the lack of evidence regarding the effect of law enforcement take-downs is not proof that there were no impact at all. Van Buskirk et al. [11] and Buxton and Bingham [10] limited their analysis to an evaluation of the level of activity on cryptomarkets that survived the police crackdown, which, per se, is not an evidence of displacement. Indeed, while some dealers may have moved to new cryptomarkets, the activity intensity of cryptomarkets may be lower compared to their pre-Operation Onymous level. Soska and Christin’s study [12] represents the sole pre-and-post analysis. However, their longitudinal analysis on the effect of police interventions on cryptomarkets focuses almost exclusively on sales volumes and dealers’ presence. Understanding the impact of police operations goes beyond the simple analysis of the level of activity of participants and needs to consider other dimensions of the supply, demand and prices of illicit drugs. Drug policy analysts have developed a mature design method to evaluate the impact of law enforcement on traditional drug markets looking at supply [44], demand [45] and prices [30]. We intend to apply this design method to Operation Onymous.

The main objective of this paper is to describe and explain the impact of police crackdowns on cryptomarkets. This impact will be measured through two dimensions. The first will be the changes in the prices, the supply and the demand for illicit drugs on cryptomarkets before and after Operation Onymous. The second will be the presence of displacement of cryptomarket participants from markets that were targeted by Operation Onymous to those that were not.

Based on past research, we expect to find stable levels of activities and prices on cryptomarkets following the Operation Onymous. Police crackdowns have shown to have little to no impact on drug market activities. The virtual setting of cryptomarkets raises questions about the applicability of research on traditional drug markets to their virtual counterparts. Décary-Hétu [46] answers some of these questions in his evaluation of the impact of multiple international and large-scale police operations targeting the community of hackers responsible for the illicit distribution of copyrighted content
online (e.g., books, software, games, and movies). Using an interrupted time series model, Décary-Hétu [46] demonstrates that there were no significant changes in the number of active hacker groups or in the number of files released online following police operations, which suggests that police operations in the physical and virtual worlds have similar outcomes.

We also expect to find a displacement of participants from markets that were shut down to markets that were not. Buxton and Bingham [10] and Van Buskirk et al. [11] already found support for this hypothesis and we intend to extend their findings by analyzing data collected from five cryptomarkets (AGORA, CLOUD-NINE, EVOLUTION, HYDRA, and SR2) during the months before and after Operation Onymous.

This paper provides a much more comprehensive overview of adaptation techniques used by cryptomarket participants and adopts a research design developed for researching the effect of law enforcement on traditional drug markets. This paper will be of interest to a broad range of criminologists interested in the impact of new technologies on offenders. Virtual settings are expanding quickly and attracting a greater share of organized crime [47]. Many offenders are joining online communities and markets (see Holt et al. [48] and Holt and Lampke [49] for examples in prostitution and computer hacking). Differences between online and offline offending are therefore likely to shrink over time. Understanding the dynamics of participation in virtual illicit markets can provide us with an interesting new methodology for understanding crime. This paper also builds on the quantitative approach of Christin [41], Aldridge and Décary-Hétu [1] and Soska and Christin [12] who have explored how virtual drug markets can be used to better understand drug trafficking in general. It goes beyond past research by analyzing cryptomarkets as an industry rather than looking at only one specific market. It also provides longitudinal quantitative-based research that allows a much more robust analysis of displacement techniques using data that is not accessible to traditional displacement studies.

Cryptomarkets provide what may be the most comprehensive dataset ever available on the impact of police operations. Past research has had to rely on controlled buys, official records, and interviews with a limited number of market participants in order to evaluate the impact of police operations. With cryptomarkets, precise evaluations of the supply and consumption for drugs on those markets can be measured automatically across time. Cryptomarkets also provide an opportunity to study the evolution of drug prices. They thus provide a unique opportunity to advance the literature on displacement, offender adaptation, and the impact of police operations. The methodology used in this paper could be used to study many of the growing online communities where johns and computer hackers meet. It could also be used to further understand some aspects of organized crime, which is increasingly moving into the virtual world [47].

Data

This study uses data collected by an independent researcher who has been actively monitoring cryptomarkets since the beginning of 2014 [50, 51]. Branwen developed his own custom monitoring tool that logged in to cryptomarkets and extracted their listings,

---

2 Johns is a generic term that describes the men looking for escorts.
dealer profiles and buyers’ feedbacks. While many small and large cryptomarkets were monitored by Branwen, we opted to focus on five of the largest cryptomarkets for this study: AGORA, CLOUD-NINE, EVOLUTION, HYDRA and SR2. Together, these cryptomarkets hosted the majority of all cryptomarket listings online and are therefore representative of the state of cryptomarkets during the sample period which ran from January 2014 to March 2015. Operation Onymous was launched on November 5, 2014 and led to the seizure of CLOUD-NINE, HYDRA and SR2. AGORA and EVOLUTION were not targeted by the police crackdown. Our dataset therefore contains data on the 41 weeks before or during Operation Onymous and the 21 weeks that followed. The dataset we received contained 1,746,737 listings and 136,963 dealer profiles, though many listings and dealers were duplicates from week to week. The dataset contained 226,297 unique listings and 7280 unique dealers.

The dataset collected by Branwen is unique in that it provides an extensive look into the activities of cryptomarkets over an extended period of time. It is however not without limitations. First, while Branwen collected some data almost every week, he did not collect all of the listings, dealer profiles and customer feedbacks that were posted each week on each cryptomarket. This is due to the well-known unreliability of websites hosted on the Tor network. As a result, Branwen only collected partial snapshots of cryptomarkets each time he launched his tool. Second, Branwen’s tool was also unable to infer, from its data collection, the total population of listings, dealer profiles and listings. It is therefore impossible to determine how incomplete each snapshot of cryptomarkets is. Lastly, Branwen’s data collection was irregular at best. There could be anywhere from 0 to 4 snapshots taken during any given week. The quality of the data varies therefore from week to week.

These methodological issues led us to aggregate all of the data on a weekly basis (from Sunday to Saturday) rather than on a snapshot basis. If data were collected more than once during a week, all of the snapshots were combined and the duplicate entries were removed. Where the information had changed during the week, the most up to date information was selected. This manipulation allowed us to compensate to a substantial extent for the unreliability of the data collection by combining multiple snapshots together. The risk that an information would be missing from our dataset was reduced though not completely eliminated. While imperfect, this dataset is still to our knowledge one of only two collections of cryptomarket data that was collected for such an extended period of time and the only one accessible to the researchers. The quality of the data also changed our research design and prevented us from building interrupted time series or means difference tests. We instead rely on long-term trends in the data which are less likely to be affected by the poor quality of the data for any given week. Our data may be somewhat biased but will still be able to show the trends in the evolution of activities and prices on cryptomarkets. All our figures also present a three-week moving average (week before, week of, week after) to reduce the noise in the data.

### Methods

Our research design is based on past research that measured the effectiveness of police crackdowns in the context of traditional drug markets. It takes into account indicators of
prices, the supply and the consumption of illicit drugs. Table 1 at the end of this section summarizes all the indicators.

**Prices**

Changes in the price of drugs is the first indicator of the impact of police crackdown on cryptomarket activities. We measured, for each listing, the variation of its price across time. To do so, we compared the price of a listing at week $n$ to the price of the same listing at week $n-1$ ($\frac{P_{n-1}}{P_n} - 1$). Since the type and weight of drugs in listings never change, we could measure whether the price of the listing had gone up or had gone down. We repeated this measure for all listings across all weeks. We then averaged the price change for each week. Listing prices that more than doubled or were cut by more than half over the course of a week were removed from the sample as these price spikes usually occurred when a dealer was out of stock and wanted to keep the listing alive while preventing customers from making a purchase that could not be filled. Significant price cuts were often the results of dealer mistakes that were captured in the scrapes before they could be corrected. Even though prices on cryptomarkets are listed in bitcoins, all prices are displayed in US dollars (USD). Data on the exchange rate was collected from Bitcoincharts.com, a well-known and respected website in the bitcoin community that archives the exchange rate for BTC-E, a leading exchange market for bitcoins. As dealers can peg the price of listings in bitcoins to specific prices in USD, we do not expect the exchange rate of bitcoins to affect the price trends.

**Supply**

The supply side indicators provide us with evidence of the impact of police crackdowns on the activities of cryptomarkets and the displacement capacity of drug dealers. Our analyses focus on the number of active dealers, the number of new dealers for each week, the total number of listings and the displacement of dealers across cryptomarkets. To improve the reliability of the analyses of supply, the names of dealers across all markets were compared using the Levenshtein distance, which calculates the number of characters that need to be changed to convert one string to another.\(^3\) All dealer names were compared to each other and those that were the closest (Levenshtein distance of 25% or less of the number of characters in the dealer name) were manually compared to make sure that they did not represent the same dealer as dealers sometimes opened accounts on different markets using different but very similar names (ex: *weed_dealer* and **weed__dealer**).\(^4\) This method allowed us tie together accounts with different names.

To measure the number of active dealers, a list of dealers was compiled from the listings (which provide the dealer’s name) and the dealer profiles. Duplicate dealer names in each week were then removed. Dealers with no feedback during a week were considered to be inactive for that week and removed from the sample. As it is easy to create a dealer profile, many dealers put up listings on cryptomarkets but

---

\(^3\) The Levenshtein distance between compute and commute is 1, as changing one character, $p$, transforms the first string into the second.

\(^4\) These are not actual dealer names but are indicative of the differences found in dealer names.
never have an actual sale, leading to an overestimation of the size of supply if we use number of available dealers. As a control measure, the proportion of active dealers was compared to the total number of dealers to detect changes or possible manipulation of the data.

We also assessed the number of new dealers on AGORA and EVOLUTION for each week between August 2014 and January 2015. We limited our analysis to these two markets as they are the only two that survived to the police crackdown. We also limited our sample period in order to focus on the trends immediately before and after the police operation. The short lifespan of dealer profiles [12] also suggested that extending the sampling period would increase noise and would include dealers that had stopped dealing for reasons unrelated to Operation Onymous.

We measured the availability of products through the number of listings posted each week on all cryptomarkets before the operation and on AGORA and EVOLUTION following it.

Finally, to test the displacement effect of Operation Onymous, we measured the number of dealers who moved to other markets following the police intervention. We classified dealers active in the five weeks leading to Operation Onymous according to three categories: 1) those selling only on cryptomarkets shut down during Operation Onymous; 2) those selling only on cryptomarkets that were not shut down during Operation Onymous and; 3) those selling on both cryptomarkets that were shut down during Operation Onymous and those that were not. Given the short lifespan of most dealer accounts [12], including all past dealers might have artificially increased the number of dealers who had stopped selling following Operation Onymous. The number of dealers in each of the three categories who continued to sell on AGORA and EVOLUTION after Operation Onymous was measured at 4 weeks, 8 weeks, and 12 weeks after Operation Onymous to detect a possible cooling down period.

It is possible that some dealers moved to physical drug markets following Operation Onymous. However, it is not possible to assess displacement to traditional drug markets or to distinguish dealers who stopped selling drugs following Operation Onymous from those who changed their dealer name but continued to sell on other cryptomarkets. Still, analysis of the displacement of those dealers we can track is likely to generate some insights into the displacement of dealers at the aggregate level.
Consumption

The consumption of drugs was measured by two indicators. The first, the number of feedbacks posted each week, was built using data on feedbacks from HYDRA, EVOLUTION, and SR2. Further feedback data were collected in dealer profiles on AGORA, CLOUD-NINE, HYDRA, and EVOLUTION. In all of these markets, dealer profiles detailed the aggregated number of feedbacks for each dealer across all their listings. To merge the two datasets, we aggregated the feedback data from the listings for each dealer for each week. We then compared this to the data from the dealer profile for the same week. If the two numbers did not match, we kept the bigger of the two. The number of feedbacks is the best proxy available for consumption of drugs on cryptomarkets. Buyers are strongly encouraged to leave feedback for each transaction and do so most of the time. Past evaluations of the correlation between the number of feedbacks and the advertised number of sales of vendors has shown a very high correlation [1]. The second indicator is the average market share controlled by dealers also referred to as the concentration of sales. To assess it, we divided the number of feedbacks of each dealer by the total number of feedbacks from all dealers on the same market. We limited our analysis to AGORA and EVOLUTION to provide a more robust comparison before and after Operation Onymous. Table 1 report the indicators that we used to understand the effect of Operation Onymous on cryptomarkets.

Results

We begin our analyses by looking at trends in drug price changes across all five cryptomarkets (AGORA, CLOUD-NINE, EVOLUTION, HYDRA, and SR2) for the 41 weeks that preceded the police operation as well as the 21 weeks that followed it. Figure 2 shows that prices did not change drastically after the operation, staying well below a 2% average price change. Prices dropped during the first weeks of the sampling period but this could be explained by the drop in price of the value of bitcoins. On some markets dealers could peg their listing price (which had to be in bitcoins) to the US dollar but not all markets had that feature enabled from the start, which could explain the drop in price. As the price of bitcoins continued to fluctuate, the impact on markets seemed to disappear. There is a slight drop in the price of listings following Operation Onymous, but this drop is not significantly different from the many others that occurred during our sampling period. Figure 2 demonstrates the stabilization of prices over time. The largest peaks and valleys are found at the beginning of the sampling period when the markets were not yet mature. Over time, the price of listings generally varies by less than 3%, a change that could be the result of having to convert the price of drugs into bitcoins.

Moving to the supply side of drug markets, Fig. 3 presents the evolution of the number of active dealers (those with at least one feedback during the prior week) over

---

5 CLOUD-NINE did not provide any feedback information in its listing pages. Listings on AGORA only presented the last 20 feedbacks, preventing us from measuring the exact number of feedbacks for each listing.

6 On EVOLUTION, the dealer profiles listed number of feedbacks up to 1500. Dealers with more than 1500 feedbacks were listed as having 1500+ feedbacks. Given the small number of dealers with 1500+ feedbacks, these dealers were removed from the datasets.
time. It shows a largely upward trend in the number of dealers in the five cryptomarkets in the period before Operation Onymous. In the period that followed Operation Onymous, the number of active dealers on AGORA and EVOLUTION registers an important drop. This drop stops in December 2014 when the number of dealers appears to increase again. The increase is particularly striking in the case of EVOLUTION, the market that contains the largest share of active dealers. At the end of the sampling

Fig. 2 Average price change of listings per week in AGORA, CLOUD-NINE, EVOLUTION, HYDRA, and SR2

Fig. 3 Number and proportion of active dealers per week on AGORA, CLOUD-NINE, EVOLUTION, HYDRA, and SR2
period, the number of active dealers appears to have risen almost to its high of October 2014, even though only two markets out of five were still active. The upward trend in the number of active dealers that began in December 2014 suggests that the number of active dealers might have surpassed its high for the year if the sampling period had been extended. The total number of dealers appears to follow a similar trend to that of active dealers. The proportion of active dealers hovers between 55% and 70% for much of the sampling period, meaning that there was no vast increase in the number of inactive dealers before or after Operation Onymous.

Figure 4 investigates the displacement impact of Operation Onymous further by presenting the number of new dealers who signed up on AGORA and EVOLUTION each week. It shows a largely upward trend in the number of new dealers on both markets before Operation Onymous, suggesting that the cryptomarkets were in an expansion phase. Following Operation Onymous, this trend is reversed and shows a decrease in the number of new dealers for the following weeks. The number of new dealers per week only increases again at the beginning of 2015.

Table 2 presents the percentage of dealers who continued to sell illicit drugs in cryptomarkets after Operation Onymous. The results show that Operation Onymous had the strongest impact on dealers of cryptomarkets that were shut down (CLOUD-NINE, HYDRA, and SR2). The first row of Table 2 shows that in the 4 weeks following Operation Onymous, only 6% of dealers who were exclusively active on markets that were shut down displaced their activity to AGORA and/or EVOLUTION. This proportion increased to 7% and 8% respectively in the 8 and 12 weeks that followed the operation, an increase that is too small to be interpreted as significant or otherwise. The proportion of dealers originally active on AGORA and EVOLUTION who stopped selling following Operation Onymous is much lower. Only 25% of dealers quit selling drugs in the 4 weeks following the police operation while 75% of them continued dealing on AGORA and/or EVOLUTION. This proportion increases to 80% and 81% in the 8 and 12 weeks following Operation Onymous. Dealers who

![Figure 4](image_url)  
*Fig. 4  Number of new dealers signing up on AGORA and EVOLUTION per week*
were active on both cryptomarkets that were shut down and those that were not continued to sell in a majority of cases (86 % after 4 weeks). This proportion increases to 89 % after 12 weeks. These results per se are not indicative of the deterrence impact of Operation Onymous. Indeed, it is still possible that dealers who appeared to have ceased their illicit activities used a tactical displacement to sell in physical instead of virtual markets. It is also possible that dealers changed their dealer name to reduce the risks of being associated with their past activities on markets that were shut down. It is possible, finally, that dealers moved to cryptomarkets other than AGORA and EVOLUTION.

Figure 5 presents the number of listings per week, a measure roughly comparable to the availability of illicit drugs in traditional drug markets. The main outcome of Operation Onymous was the elimination of the listings on CLOUD-NINE, HYDRA, and SR2. The impact on AGORA and EVOLUTION appears to be marginal. Indeed, while the total number of listings available in cryptomarkets dropped in the weeks immediately following the operation, the number of listings in the remaining markets remained stable. This suggests that Operation Onymous was unable to substantially affect the availability of drugs on cryptomarkets. Indeed, even though the total number of listings decreased, the large number of listings still online probably offered enough supply to satisfy all potential customers.

Moving to the consumption side of cryptomarkets, Fig. 6 presents the evolution of the number of feedbacks per week, a proxy for the number of sales on AGORA, CLOUD-NINE, EVOLUTION, HYDRA, and SR2. Until Operation Onymous, the number of

<table>
<thead>
<tr>
<th>Table 2 Displacement of dealers across cryptomarkets after Operation Onymous</th>
</tr>
</thead>
<tbody>
<tr>
<td>Still selling X weeks after Operation Onymous</td>
</tr>
<tr>
<td>Dealers from markets that were shut down</td>
</tr>
<tr>
<td>Dealers from markets that were NOT shut down</td>
</tr>
<tr>
<td>Dealers from both types of markets</td>
</tr>
</tbody>
</table>

Fig. 5 Number of listings per week on AGORA, CLOUD-NINE, EVOLUTION, HYDRA and SR2
feedbacks posted each week continued to increase. Operation Onymous appears to have a chilling effect on sales, as the number of feedbacks drops between the week of November 3, 2014 and the week of December 29, 2014. The effect of the operation extended beyond CLOUD-NINE, HYDRA, and SR2, reducing sales on AGORA and EVOLUTION for the period between November 3 and December 29. Figure 6 demonstrates the presence of a nine-week cooling down period during which the number of sales appears to decrease. Starting in the first week of 2015, the number of feedbacks per week rebounds, however, eventually surpassing by far the number of feedbacks posted before Operation Onymous. This growth is particularly evident in the case of Evolution, which moves to account for about 72% of all feedbacks.

Finally, Fig. 7 shows the average concentration of feedbacks for dealers on AGORA and EVOLUTION as well the number of active dealers for the two markets. This figure shows data for the period between the weeks of July 14, 2014 and March 14, 2015. Unlike the previous figures, we do not report values for the first half of 2014 because the spikes in this period would add noise to the trend that follows Operation Onymous. Indeed, between January and June 2014, values on the concentration of sales show an unstable trend, with spikes and valleys ranging between 0.1% and 0.8%. However, beginning in July 2014, concentration of feedbacks is quite stable, though decreasing. Operation Onymous stopped this decreasing trend, changing the slope of the curve and stabilizing the concentration of sales around 0.1%. This indicates that the operation affected the behaviour of buyers, who, in response to it, concentrated their purchases with a lower number of dealers.

The trend for the whole time series (from January 2014 to March 2015) suggests that after an initial period where a few dealers captured a larger share of feedbacks, the number of buyers, dealers, and sales increased, leading to higher competition and a smaller market share for dealers in general. As we saw with drug price changes,
Cryptomarkets appear to stabilize in the weeks that lead to Operation Onymous. The police operation affected this equilibrium.

**Discussion**

Our results demonstrate, first and foremost, the diffusion of the benefits of Operation Onymous. The operation, though directed at CLOUD-NINE, HYDRA, and SR2, impacted the supply and consumption of drugs on AGORA and EVOLUTION. Indeed, in the weeks that followed Operation Onymous, the total number of dealers and the number of new dealers who registered on AGORA and EVOLUTION each week dropped. Furthermore, the vast majority of dealers on markets that were shut down did not displace to AGORA and EVOLUTION. A much smaller number of dealers on markets that were not targeted also quit selling. On the consumption side, the number of sales (as estimated by the number of feedbacks) also dropped.

While impressive at first, these results are offset almost completely when we look at the impact of Operation Onymous over the longer term. The number of active dealers recovered to almost its pre-operation level within a month; the number of new dealers per week took a bit longer, at two months. On the consumption side, the number of sales appeared to be twice as high two months after Operation Onymous as it had been before. Our results, in line with past research on physical drug markets [23, 25, 27, 28], demonstrate that the police operation had a deterrent effect but one that was limited in time to one or two months.

Buxton and Bingham [10] and Van Buskirk et al. [11] have suggested that police operations could actually be beneficial for cryptomarkets in general as they increase awareness of the virtual drug markets among drug users and dealers. Such an impact is not apparent in our results. The rate at which new drug dealers entered the markets was lower in the follow-up period than in the period before Operation Onymous. The

---

**Fig. 7** Concentration of feedbacks per week and number of active dealers per week on AGORA and EVOLUTION
number of active dealers was also lower. On the consumption side, the number of sales (as measured by feedbacks) vastly increased in the months that followed Operation Onymous. It is not possible at this point to distinguish between the effect of an increased awareness of cryptomarkets among drug users and the organic growth that cryptomarkets had been experiencing before the police operation. The creation of the Tor browser has vastly improved the ease of access to cryptomarkets but there are still technological challenges, such as the management of bitcoins, which market participants have to solve before they can become active participants. These technological hurdles could explain the lack of impact of the publicity or the month or two delay between the publicity associated with Operation Onymous and the rise in sales.

More surprising was our finding that Operation Onymous was able to deter almost all of the active dealers in CLOUD-NINE, HYDRA, and SR2. Indeed, only a very small fraction of dealers who were selling on these markets displaced to AGORA and EVOLUTION. This does not indicate per se that dealers stopped dealing in illicit drugs. Dealers could have changed their dealer name, moved to other cryptomarkets, or simply stopped selling online (but continued to sell in / move to physical markets). Testing either of these hypotheses is beyond the scope of this paper but suggests that virtual dealers are, just like physical drug dealers, more risk-averse than profit-oriented [15, 52]. It is possible that, in their view, the risk associated with their dealer name exceeded the profits they could generate through their established reputation. This is somewhat surprising, given the low risk of arrest of dealers, even following a major police operation [53]. Of course, it is also possible that dealers waited more than the 12-week follow-up period of this study to transfer their accounts to the new markets.

Regarding the prices of drugs before and after Operation Onymous, there is no evidence that prices increased following Operation Onymous, despite the assumptions of the Risks and Price model [15]. Indeed, it seems that while a portion of dealers stopped selling, those that kept on selling did not raise their prices. This suggests that the perception of risks by dealers who continued to sell remained the same. It may also suggest that dealers were not able to take advantage of the reduced level of competition following Operation Onymous by increasing their prices or gaining a greater control over the market. As in physical drug markets, dealers in cryptomarkets are “price-takers rather than price-givers” ([54]: 67). An alternative explanation is that dealers sought to preserve the loyalty of their customers by maintaining their prices at the same level. The risk analysis of dealers who continued to sell appears to be different than that of dealers who stopped selling following Operation Onymous. Indeed, though we were unable to track all of them, some dealers apparently perceived risks to be so high that they decided to stop selling online. A last explanation would be that the dealers did not change their listings but instead changed the product they shipped. Dealers could cheat their customers by sending smaller weights than advertised or by reducing the amount of active ingredients in their drugs. This technique would have the benefit of keeping the prices at the same level and of increasing the dealers’ profits to match the new level of risks. Further investigation will be needed to better understand how and why the perception of risks of dealers varies in time and whether changes in the level of satisfaction of buyers could be used to detect adaptation techniques that cheat customers.

Just as in a traditional drug market, buyers in cryptomarkets adapted to the increased level of enforcement through tactic displacement. Indeed, in the weeks following the
operation the concentration of sales show almost opposite trends. As a consequence of the higher perception of risk of being arrested by law enforcement agencies, buyers in cryptomarkets adapted, concentrating their purchases with a lower number of dealers. As open drug markets have often turned into closed ones [24, 32, 33], cryptomarket participants may adapt to a police crackdown by concentrating their transactions with fewer but trusted dealers. The possibility of safely adapting to the higher level of enforcement may explain why Operation Onymous was less effective against buyers than dealers. Indeed, the drop in the volumes of sales per week after the operation is less pronounced than the fall in the number of active dealers.

This discussion on the average price change and the rapid recovery of cryptomarkets highlights the maturity of virtual illicit drug markets. According to most measures, it appeared to be business as usual on AGORA and EVOLUTION two months after the police operation. Furthermore, there was no decline in the number of listings on AGORA and EVOLUTION and no increase in prices, even though the number of dealers decreased. Another indication of the maturity of cryptomarkets is the stabilization of the concentration of sales following Operation Onymous. The average market share of dealers was much higher in the first months of 2014 but dropped continuously until Operation Onymous. This is a surprising result as cryptomarkets in general are a fairly new phenomenon and the markets that were affected by Operation Onymous (directly or indirectly) were all less than one year old. Such a finding demonstrates the power of new technologies to create communities and to ease adaptation. Two decades ago, technology had already been cited as a driving force in the transition from open to closed drug markets [24, 32, 33]. Technology, it now seems, is responsible for the creation of a new breed of open markets that offer much improved security for all participants. The main consequence of Operation Onymous seems to have been a chilling effect on the stable growth in the volume of sales, flattening the trends in the weeks between November 3 and December 29.

Conclusions

This paper focuses on the impact of police crackdowns on cryptomarkets. Our results demonstrate that Operation Onymous affected participants but only for a short time. Both the supply of and the consumption of drugs were impacted, though drug prices appear to have remained unchanged. The operation had an effect beyond the markets that were shut down, affecting also AGORA and EVOLUTION. Only a small percentage of dealers made use of “geographic” displacement by moving to alternative cryptomarkets after Operation Onymous, while buyers used tactical displacement, concentrating their purchases with fewer, and probably more reliable, dealers.

Our results indicate that police crackdowns, as is the case for traditional drug markets, are not effective measures to lower the volume of sales on online illicit drug markets. Cryptomarket participants have been shown to have a minimal reaction, or one that is temporary, to overtly large shows of force and to have the ability to adapt through displacement techniques. Investing time and resources into the seizure and take down of cryptomarkets therefore appears to be an ineffective way to enforce drug laws on the Internet, whatever their symbolic value to enforcement and to politicians of showing that something is being done. Other approaches could be investigated by law
enforcement, including the targeting of key participants and the disruption of trust. Soska and Christin [12] explain that a small fraction of dealers are responsible for a large portion of the sales. By targeting these individuals, law enforcement would force a large number of participants to find new suppliers and to build up trust again with new dealers. Much of the benefits of cryptomarkets come from the feedbacks and reputation systems cryptomarkets use. Past research [55] has shown that attacks that target reputation systems could be used to destabilize online illicit markets and disrupt their activities.

Future research should look into the impact of such law enforcement techniques on the activities of cryptomarkets and online illicit markets. The growing number of law enforcement operations on the Internet should provide interesting case studies in the years to come. Future research should also expand the research on cryptomarkets, a prime example of a criminal activity that has transitioned from the physical to the virtual world. Examining the structure of cryptomarkets and the operations of their participants provides new insights on how drug markets are organized, making it possible to provide answers to previously raised questions. Of most interest for further research are the evolution of drug prices and the differences between national dealers. Anecdotal evidence suggests that dealers in different countries sell different types of drugs and at different price points. Cryptomarkets can provide the data researchers need to look at use patterns and drug penetration in countries around the world.

The main limitation of this paper comes from the quality of the data that was collected by Branwen. Soska and Christin [12] faced similar challenges when collecting data on a massive scale on cryptomarkets. Through our careful approach, we sought to minimize the uncertainty of the representativeness of the data by aggregating data on a weekly basis and by looking at long-term trends. By doing so, we reduced the week-to-week variations and managed to identify trends in the dataset. Another limitation of this paper is the relatively short follow-up period and the dynamic nature of cryptomarkets. Time series analyses usually require that a full cycle be analyzed before and after an event. Given that the operation occurred less than a year before we wrote this paper, it was not possible in this case to conduct more rigorous statistical analyses of the data. Our goal was to provide an overview of the impact of Operation Onymous and future studies should look into the longer-term impact of the law enforcement operation. This task will be made difficult by the constantly changing nature of cryptomarkets. New cryptomarkets are created every month and participants may move from one market to another. Separating the impact of a police operation from the natural expansion and contraction of cryptomarkets will be a daunting task that should be achieved by incorporating more qualitative analyses from interviews and observation of participants’ discussions on online forums. Doing so will provide a more in-depth understanding of the reaction of cryptomarket participants and the impact that anonymity and the Internet have on police crackdowns.

References


Cyberfraud and the implications for effective risk-based responses: themes from UK research

Michael Levi1 · Alan Doig2 · Rajeev Gundur3 · David Wall4 · Matthew Williams5

Published online: 20 October 2016
© Springer Science+Business Media Dordrecht 2016

Abstract The nature of the risk or threat posed by ‘cyberfraud’ - fraud with a cyber dimension – is examined empirically based on data reported by the public and business to Action Fraud. These are used to examine the implications for a more effective risk-based response, both by category of fraud and also responding to cyberfraud generally, not just in the UK. A key characteristics of cyberfraud is that it can be globalised, unless there are major national differences in attractiveness of targets or in the organisation of control. This does not mean that all cyberfraud is international, however: not only do some involve face to face interactions at some stage of the crime cycle, but in online auction selling frauds, it appears to be common for the perpetrators and victims to reside in the same country. After reviewing patterns and costs of victimisation and their implications for control, the paper concludes that any law enforcement response must begin by being strategic: which other public and private sector bodies should be involved to do what; what should be the specific roles and responsibilities of the police and where ‘problem ownership’ should lie; what are we willing to pay for (in money and effort) for greater cybersecurity and how to reduce ‘market failure’ in its supply; and, how that security is going to be organised for and/or by the huge numbers of businesses and people that are (potentially) affected.

We are grateful to the City of London Corporate for funding this research and to the City of London Police and Steve Strickland for their substantial assistance with the project.

Michael Levi
Levi@Cardiff.ac.uk

1 School of Social Sciences, Cardiff University, Wales CF10 3WT, UK
2 Northumbria University, Newcastle upon Tyne, UK
3 Social Policy and Criminology, University of Liverpool in Singapore, Singapore, Singapore
4 Centre for Criminal Justice Studies, Leeds University, Leeds, UK
5 School of Social Sciences, Cardiff University, Cardiff, UK
Introduction

This article looks specifically at the nature of the risk or threat posed by ‘cyberfraud’, fraud with a cyber dimension. By examining cybercrime for financial gain, it will seek to develop an outline of the implications for a more effective risk-based response, both by category of fraud and also responding to cyberfraud generally. While the dataset upon which this article draws relates to England and Wales, the article is not focussed exclusively on those countries, but upon what the authors suggest are the main risks and threats in any context experiencing an increase in cyberfraud and the steps needed to enhance the effectiveness of risk-based responses. One of the key characteristics of cyberfraud is that it can be globalised, so what is found in one jurisdiction tends to also be found in another, unless there are major national differences in attractiveness of targets or in the organisation of control. This does not mean that all cyberfraud is international, however: not only do some involve face to face interactions at some stage of the crime cycle, but in online auction selling frauds, it appears to be common for the perpetrators and victims to reside in the same country.

Financial and other risks and threats to current and future ‘Internet of Things’ and ‘Big Data’ processes in the ‘cyber’ world are ever present and constantly evolving (see [1]). Regular national and global cyber ‘threat assessments’ and state-wide Cyber Security Strategies add to the ‘awareness-raising’ process that puts the probabilities or impacts of certain forms of victimisation on the public agenda with varied degrees of sophistication [2]. Action (pre and post-victimisation) increases demands on law enforcement for resources for investigation and prosecution (while also enhancing the sales of the cybersecurity businesses that have been spawned by the rise of e-commerce and social media).

In this market for understanding threat, risk, and effective responses, it is difficult for most consumers, businesses, government organisations, and commentators to work out a ‘rational’ response or responses, not least because there is a lack of reliable data on the problem, and little helpful agreed evidence on ‘what works’ and on who has both the capacity and the motivation to reduce vulnerability [3]. Moreover, given the often transjurisdictional nature of cyberfrauds, there is difficulty in acting against perpetrators, especially because both vulnerabilities and perpetrators are dynamic and responses need regular updating in order to be focused and effective. A key challenge has been the lack of accurate data and measurement of the nature, scale and impact of cyberfraud, largely due to the relatively recent emergence of cybercrime on the criminal justice agenda and its poor capture in existing crime surveys and datasets [4]. Nonetheless, it is arguable that there is a significant risk that law enforcement and other resources target the wrong crimes, fail to instil confidence in victims and potential victims in their ability to prevent cybercrime from occurring or are unable to respond effectively because of the nature of the crime and the lack of a suitable evidence base for assessing impact. Indeed, there is often confusion over whether any guardianship component or mix of components of reassurance policing, target hardening, enhancing resilience, or pursuing offenders constitutes ‘effective policing’ of cyberfrauds [2].
The optimal enforcement response is also influenced by changes to crime control in the UK which was once widely seen as virtually the sole domain and responsibility of law enforcement, but which in the past two decades has moved towards ‘plural policing’ in partnership with other agencies [5]. This shift has resulted in a new emphasis on partnership and information-sharing; between and across jurisdictions; the framing of responses to crime in terms of prioritising on the basis of harm, disruption, prevention and reduction; the production of explicit and measurable policies, strategies or ‘policing plans’ which are themselves ostensibly the result of analyses of crime patterns and trends; the application of intelligence-led policing; and the consideration of the priorities of central and local government, other agencies and local communities [6, 7]. Levi & Williams [8] in their study of cooperation within the UK Information Assurance Network evidence that the neo-liberal rationality that has been evoked in other areas of crime control is also evident in the control of cybercrimes. However, they find divisions exist between the High Policing rhetoric of the UK’s Cyber Security Strategy and the (relatively) Low Policing cooperation outcomes in “on the ground” cyber-policing.

In the area of fraud, which also includes cybercrime for financial gain, similar imperatives also apply in terms of law enforcement responses to the public, as well as public and private sector institutions, who may approach law enforcement with allegations of criminal conduct or financial loss. An awareness of investigation policies and the reduced availability of resources within the police service, other institutions and regulators, as well as a requirement to follow a broad range of government-initiated policies has seen the police commit ever-fewer resources to high-volume, low value cases. This also applies the more elite forms of fraud such as insider trading and corporate accounting frauds. The shortfall in resources raises questions as to the extent to which the police are able to address the growing threat from cybercrime for financial gain, which has long been a problem for fraud generally [6, 9, 10].

**Establishing an evidence base**

Given the lack of resources available for responding to cybercrime in general and cybercrime for financial gain in particular, we must continuously develop our understanding of the range of risks or threats facing victims – corporate, governmental or individual - and tailor roles and responses accordingly, to the extent that there are sufficient resources to fulfil those roles. To that end, identifying the evidence base on which to predicate law enforcement roles as well as responses of those of other organisations (including the relevance and added-value of cybersecurity businesses) is necessary in order to develop an effective response.

Some data about offenders can be derived from investigating the circumstances and techniques for criminal activity (see this volume), but the evidence is inadequate to test the hypotheses that, for example, cybercriminals are more financially motivated than in the past when they were more likely to be motivated by gaining kudos; or that traditional, analogue criminals – particularly drug traffickers, burglars and robbers – are digitizing their offending habits by turning to the more sophisticated forms of cybercrime in significant numbers, beyond what can be done comparatively easily from ‘crime-as-a-service’ software kits [11, 12]. There has also been little evidence on the
relationships between types of crime, losses incurred, or the nature and level of cyber involvement; certainly police recorded data have been poor and/or partial in their coverage, leaving little scope for credible refutation of hostile media stories about cybercrime risks and bank/police handling of complaints. Currently criminal statistics as well as business and individual victim surveys show that fraud in the UK is on the rise, while the crime rates for other types of acquisitive crime are falling. However, the evidence base for how ‘cyber’ has contributed to fraud has been incomplete and weak, both today and historically. Since ICT platforms have become central to the way business and social life is organised, routine activities models lead us to expect that crime follows these changes when the opportunity is easily exploitable.

A much more detailed picture of UK cyberfraud has recently emerged as a consequence of improved law enforcement reporting arrangements (which is patchily present in other countries also). In the UK, following a review of the UK institutional approach to fraud, there is now a centralised reporting process for all actual and attempted fraud allegations, including those involving a cyber dimension. However, the effectiveness of this process is dependent on victims’ awareness that they have been defrauded and willingness to spend the time making reports. The review recommended that there should be a National Fraud Reporting Centre as a sole central reporting point for members of the public and both public and private sectors ([13]: 7). This body is located within the City of London Police, which was designated as the national lead law enforcement agency responsible for policing fraud.

Currently renamed ‘Action Fraud’, the Centre was linked to an intelligence analysis resource: the National Fraud Intelligence Bureau (NFIB), also located with the City of London Police. In 2013, Action Fraud was rolled out nationally. Since 2014 all fraud complaints to the police, unless an immediate response is required for a ‘crime in action’, have to be recorded through Action Fraud and not locally. Action Fraud collects data for reported frauds by UK individuals and businesses, excluding reports for ‘plastic crime’ which is collected by CIFAS and FFA UK, to avoid double counting.¹ The former is a member-based fraud prevention service while the latter coordinates information from, and preventative approaches for, some sectors of the financial services industry. The NFIB role has been to synthesise and analyse the data from these three sources in order to assess patterns and trends, as well as directing intelligence packages to the most relevant police force, although it has no control over what those individual forces do with its packages, an issue in common with other police intelligence bodies including CIFAS and FFA UK.

For a research project intended to explore the implications of economic cybercrimes for a law enforcement response [11], the authors were given access to Action Fraud data for all fraud and fraud-related offences, including offences recorded under the 2006 Fraud Act and 1990 Misuse of Computers Act, for October to December 2014. This analysis of the reported cyber dimension of fraud enabled a detailed picture to be drawn of the types of frauds reported and, with access to the reporting information, the

¹ For 2013–14 CIFAS and FFA UK sent to the NFIB data on ‘card not present’ fraud, lost or stolen cards and ATM fraud, representing over two-thirds of the total of over 333,000 reported offences and, while most will involve a cyber dimension, the data are not differentiated in the same way as Action Fraud data. This will continue to be the case despite the integration of those commercial sources into the crime statistics (see Levi, this volume).
mode of commission of the alleged crime to assess the issues faced by law enforce-
ment, organisations and the public.²

What is cyberfraud and what is the ‘cyber’ component thereof?

There is a distinction between cybercrime intended solely to harm – such as online
harassment, hate speech and child sexual grooming – and cybercrime for financial gain,
including cyberfrauds and extortion. There are three main aspects of cybercrime in
relation to fraud [14]:

- **Cyber-dependant crimes** which would not exist without the internet;
- **Cyber-enabled crimes** which, if the networked technologies were removed, could
still take place but locally and on a more one-to-one basis. Being cyber-enabled
allows these crimes to be carried out at scale for less capital and sometimes with
fewer criminal staff than would be needed for similar crimes offline; and
- **Cyber-assisted crimes** which use networked digital technologies in the course of
criminal activity which would take place anyway.

In focussing particularly on the latter two dimensions of cyberfraud (as the data will
show, cyber-dependent crimes are not the main source of cybercrime for financial gain),
one of the questions also addressed through the data in seeking to identify where the
cyber element occurs, in what forms at any stage, from the planning of a crime through
to its execution, to the expenditure and/or laundering of its proceeds.

What is the scale of, and the threat from, cyberfraud in the UK?

This study preceded the extension of the national statistics to cover a broader range of
cyber-related frauds in England and Wales (ONS [15]; Levi, this volume). Overall,
there were 106,681 reported incidents in the dataset provided to the authors by Action
Fraud³ - of these, 4062 (4 %) involved computer misuse crime, a much smaller
proportion than might have been expected, perhaps because people whose systems
become infected by malware do not bother calling Action Fraud, if indeed they are
aware of it and see it as a prelude to fraud against themselves or others. The two largest
components of computer misuse crime involved malware, and hacking of emails and
social media.

The analysis of the data suggested that well over half of incidents were significantly
cyber-related: 43 % were cyber-enabled, 13 % were cyber-dependent, while a further
29 % of them simply used technology (cyber-assisted); see Table 1.

² The analysis of the data was supplemented with interviews with principal agencies for economic crime
control, financial services and industrial firms, cybercrime prevention bodies in the public and private sectors,
and police officers (retired and current) across the UK.
³ There are some inconsistencies in the Action Fraud data relating to the total number of cases; this is due to
missing data although totals match up closely wherever possible. It is also worth highlighting that the analysis
presented in this report is not comparable to official ONS analysis due to different datasets covering different
time periods.
By volume, the single largest types of reported fraud are banking and credit industry frauds (33 %), a large proportion of which (18 %) are cheque, payment card and online bank account frauds. This is followed by non-investment frauds (28.6 %), which include online shopping and auctions (11.6 %) and also computer software service frauds (7.9 %). The latter, which may be categorised as cyber-dependent crimes, may include, for example, fake antivirus and ransomware fraud. Advance fee frauds (and their different forms) follow (14.1 %). Specific technology-related offences are less prevalent, covering telecom industry fraud (misuse of contracts) at 4.5 %. The remainder of the offences are relatively small in volume.

Table 2 presents data for reported crime by volume by category (including the two largest sub-categories within each).

Analysis of the reporting information suggests that, despite the global figures in Table 2, the cyber dimension is much more nuanced. The data highlights that the internet has not always been the source or medium of the initial contact that led to a fraud. The single most common way that offenders first contacted their victims was by phone or text (35 %). Almost a fifth (18 %) were contacted after visiting a website, 12 % in person, letters and fax (11 %) and 8 % by email. From these data, the overall

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Cyber-involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Numbers</td>
</tr>
<tr>
<td>Cyber-assisted</td>
<td>30,759</td>
</tr>
<tr>
<td>Cyber-enabled</td>
<td>45,293</td>
</tr>
<tr>
<td>Cyber-dependant</td>
<td>13,859</td>
</tr>
<tr>
<td>Not applicable</td>
<td>16,773</td>
</tr>
<tr>
<td>Total</td>
<td>106,681</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2</th>
<th>Typology of reported frauds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud type</td>
<td>Number of frauds</td>
</tr>
<tr>
<td>Banking and credit industry fraud</td>
<td>34,913</td>
</tr>
<tr>
<td>Cheque, plastic card and online bank accounts (not PSP)</td>
<td>19,127</td>
</tr>
<tr>
<td>Application fraud (excluding mortgages)</td>
<td>10,091</td>
</tr>
<tr>
<td>Non-investment fraud</td>
<td>30,490</td>
</tr>
<tr>
<td>Online shopping and auctions</td>
<td>12,405</td>
</tr>
<tr>
<td>Computer software service fraud</td>
<td>8455</td>
</tr>
<tr>
<td>Advance fee payments</td>
<td>15,065</td>
</tr>
<tr>
<td>Other advance fee frauds</td>
<td>7498</td>
</tr>
<tr>
<td>Lender loan fraud</td>
<td>2078</td>
</tr>
<tr>
<td>No identified category</td>
<td>12,404</td>
</tr>
<tr>
<td>Categories as % of total</td>
<td>92,872</td>
</tr>
<tr>
<td>Total</td>
<td>106,681</td>
</tr>
</tbody>
</table>
degree of involvement of network technologies can be estimated, though with some caveats, and are summarised in Table 3.

The data prima facie suggest that frauds using networked technologies are actually relatively low as a proportion of the total of frauds reported. However, it is likely that the data actually underestimate the extent of cyber-involvement throughout the crime, because the data derived from the reporting stage reflect only first contact by the offender. Also, many cyberfrauds are ‘micro-frauds’, very small impact bulk victimisations that are too small individually to pursue, even if reported ([16]:68). It was also found that whilst many economic crimes involve a cyber-element at a particular point, for example emails or phone calls generated via voice over internet protocol (VOIP) might be used to make initial contact and ‘hook’ a victim, after which the fraudster will take over and monetise the victim’s personal information. Subsequently, it is not always clear for Action Fraud classifiers, or indeed for reporting victims, when the fraud actually began or at what point the cyber component occurs. This relates to a wider challenge of defining fraud. Is it at the point of initial contact, or later on when an attempt to extract money takes place? This is different from the distinction between attempted and realised fraud; some victims are carefully groomed and often will not realise that they have been defrauded until after the event, if at all.

Nevertheless, the data do provide a clear indication of the different levels of cyber-involvement in the different offences although, at this point, they do not reveal the role played by ICT in the offences: this can only be seen when it is cross-tabulated by fraud type. In the early stages of Action Fraud, reported offences that use networked technologies are relatively rare. When the data are ordered according to the level of estimated cyber-involvement, they cut across a number of the Action Fraud data headings: see Table 4. The data – which are reported quite fully to emphasise the variations by crime type of frauds other than cyber-dependent ones – allow us to assess the degree of estimated cyber-involvement for specific types of fraud and help to better understand where ICT is involved. However we caveat that the judgements about cyber-involvement made by victims or report classifiers should be treated with substantial reservation.

Thus, on the one hand, if a targeted response is being considered from the data, then traditional ‘419’ advance fee payment frauds are found to be very low in cyber-involvement (15 %), whereas others, such as dating/romance scams (88 %) and online shopping and auctions (86 %) have the largest cyber component. But the data have limitations. So, within advance fee payments, the first contact method for lottery scams suggests 8 % cyber-involvement; dating scams involve fewer cases but suggest 88 % cyber-involvement; lender loan fraud represents nearly 14 % of all advance fee payments, but only 17 % cyber-involvement on first contact method. Furthermore, it is not

---

4 Percentages are indicative rather than absolute, and are adjusted for cyber-involvement (email + visit to a website + web forum + (0.66) of TV, radio or online advert, or flyer) (‘in person’ and ‘other’ have been excluded). Classification depends on when the victim feels the fraud began, e.g. at first contact, or the point at which money was being requested. With most frauds today, online usually goes offline to get the money. Blanks are excluded and percentages are based upon total known information. ‘Simplified’ means main offence and information are joined. As the table illustrates, the Action Fraud headlines format is not very useful in demonstrating cyber-involvement.

5 Our analysis orders the fraud types in terms of cyber-involvement via first contact. Including all of the types of cybercrime (assisted, enabled, and dependent), it is calculated from the combination of the following values (email + visit to a website + web forum + (0.66) of TV, radio or online advert, or flyer) (‘in person’ and ‘other’ have been excluded).
immediately apparent which offences are cyber-enabled and which are cyber-dependent. Data are insufficient to develop horizontal or vertical analyses of perpetrators, specialisms, networks or interactions, or information sources for exploitation, although repeat victimisation requires such networks.

From the Action Fraud data, however, it is also possible to identify which types of fraud are most lucrative for the fraudster, especially where the most money is lost by the victim. Although it is worth noting that to generate criminal profits data we would have to know about operational costs to offenders and how many victims over what period they had defrauded, which might span several jurisdictions. In many cases, even with criminal network analysis software, it is unlikely that this information can be deduced from victimisation data alone, unlinked to identified (but not necessarily caught or convicted) offenders. It is, however, possible to calculate the median financial losses by the main categories of fraud: medians generate less distortion of the data than the figures alone or means, though there is still potential for inaccuracies. These victim cost data are presented in Table 5.

The data in the Table reveal that the most money was lost by corporate rather than by individual victims through pension fraud, business trading fraud, financial investments, and bankruptcy and insolvency fraud. On the other hand, more reported cases have individual than business victims. There is no clear relationship between the volume of cases and the value of financial losses, nor between those involving individuals and organisations. Nor is there a clear relationship between either of these and the level of cyber-involvement in a fraud.

The data provide some useful graded indications of the self-assessed impact of fraud upon the victim, enhance our understanding of the victims’ perspectives and thus helps

<table>
<thead>
<tr>
<th>Table 3 Frauds by first contact method by offender</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact method</td>
</tr>
<tr>
<td>Phone call, text message or similar</td>
</tr>
<tr>
<td>Visit to a website</td>
</tr>
<tr>
<td>Other</td>
</tr>
<tr>
<td>In person</td>
</tr>
<tr>
<td>Letter or fax</td>
</tr>
<tr>
<td>Email</td>
</tr>
<tr>
<td>Web forum, chat room or similar</td>
</tr>
<tr>
<td>TV, radio or online advert, or flyer</td>
</tr>
<tr>
<td>Newspaper, magazine</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

6 The City of London police graded self-assessed harm into the following categories: a) ‘Concerned about the fraud but it has not impacted on health or financial well-being’; b) ‘Minor - only a small impact on either health or financial well-being’; c) ‘Significant - impacting on health or financial well-being’; d) ‘Severe - have received medical treatment as a result of this crime and/or at risk of bankruptcy’. There is an ‘other’ category, which is where the impact is either unknown or not deemed relevant to reporting the case.
Table 4 Level of cyber-involvement in cyber-enabled and cyber-assisted frauds (Offender First Contact Method)

<table>
<thead>
<tr>
<th>Action Fraud category/sub-categories</th>
<th>Total</th>
<th>Cyber-involvement</th>
<th>% of Cyber-involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dating scam</td>
<td>835</td>
<td>737</td>
<td>88 %</td>
</tr>
<tr>
<td>Online shopping and auctions</td>
<td>11,350</td>
<td>9754</td>
<td>86 %</td>
</tr>
<tr>
<td>Counterfeit cashiers’ cheques</td>
<td>559</td>
<td>428</td>
<td>77 %</td>
</tr>
<tr>
<td>Rental fraud</td>
<td>773</td>
<td>572</td>
<td>74 %</td>
</tr>
<tr>
<td>Ticket fraud</td>
<td>910</td>
<td>655</td>
<td>72 %</td>
</tr>
<tr>
<td>Mandate fraud</td>
<td>966</td>
<td>520</td>
<td>54 %</td>
</tr>
<tr>
<td>Mortgage related fraud</td>
<td>144</td>
<td>69</td>
<td>48 %</td>
</tr>
<tr>
<td>Fraudulent applications for grants</td>
<td>9</td>
<td>4</td>
<td>44 %</td>
</tr>
<tr>
<td>from charities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business trading fraud</td>
<td>124</td>
<td>38</td>
<td>31 %</td>
</tr>
<tr>
<td>Other regulatory fraud</td>
<td>72</td>
<td>22</td>
<td>31 %</td>
</tr>
<tr>
<td>Prime bank guarantees</td>
<td>12</td>
<td>3</td>
<td>30 %</td>
</tr>
<tr>
<td>Other consumer non-investment fraud</td>
<td>4703</td>
<td>1358</td>
<td>29 %</td>
</tr>
<tr>
<td>Fraud by failing to disclose</td>
<td>160</td>
<td>46</td>
<td>29 %</td>
</tr>
<tr>
<td>information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pension fraud by pensioner (or their estates)</td>
<td>7</td>
<td>2</td>
<td>29 %</td>
</tr>
<tr>
<td>Charity fraud</td>
<td>238</td>
<td>63</td>
<td>27 %</td>
</tr>
<tr>
<td>Insurance broker fraud</td>
<td>39</td>
<td>10</td>
<td>26 %</td>
</tr>
<tr>
<td>Pyramid or Ponzi schemes</td>
<td>164</td>
<td>38</td>
<td>24 %</td>
</tr>
<tr>
<td>Other fraud</td>
<td>11,553</td>
<td>2250</td>
<td>19 %</td>
</tr>
<tr>
<td>Cheque, plastic card and online bank accounts (not PSP)</td>
<td>13,437</td>
<td>2449</td>
<td>18 %</td>
</tr>
<tr>
<td>Consumer phone fraud</td>
<td>352</td>
<td>61</td>
<td>18 %</td>
</tr>
<tr>
<td>Fraudulent applications for grants</td>
<td>41</td>
<td>7</td>
<td>17 %</td>
</tr>
<tr>
<td>from government funded organisations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other financial investment</td>
<td>1017</td>
<td>170</td>
<td>17 %</td>
</tr>
<tr>
<td>Bankruptcy and insolvency</td>
<td>18</td>
<td>3</td>
<td>17 %</td>
</tr>
<tr>
<td>HM Revenue and Customs (HMRC) fraud</td>
<td>6</td>
<td>1</td>
<td>17 %</td>
</tr>
<tr>
<td>Lender loan fraud</td>
<td>1929</td>
<td>319</td>
<td>17 %</td>
</tr>
<tr>
<td>Other advance fee fraud</td>
<td>6794</td>
<td>1017</td>
<td>15 %</td>
</tr>
<tr>
<td>Inheritance fraud</td>
<td>743</td>
<td>109</td>
<td>15 %</td>
</tr>
<tr>
<td>‘419’ advance fee fraud</td>
<td>550</td>
<td>80</td>
<td>15 %</td>
</tr>
<tr>
<td>Door to door sales and bogus tradesmen</td>
<td>1242</td>
<td>170</td>
<td>14 %</td>
</tr>
<tr>
<td>Banking and credit industry fraud</td>
<td>3637</td>
<td>495</td>
<td>14 %</td>
</tr>
<tr>
<td>fraud – information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Share sales or boiler room fraud</td>
<td>387</td>
<td>44</td>
<td>11 %</td>
</tr>
<tr>
<td>Dishonestly retaining a wrongful credit</td>
<td>32</td>
<td>3</td>
<td>11 %</td>
</tr>
<tr>
<td>Corporate procurement fraud</td>
<td>33</td>
<td>3</td>
<td>9 %</td>
</tr>
<tr>
<td>Pension fraud committed on pensions</td>
<td>24</td>
<td>2</td>
<td>8 %</td>
</tr>
<tr>
<td>Insurance related fraud</td>
<td>253</td>
<td>20</td>
<td>8 %</td>
</tr>
<tr>
<td>Lottery scams</td>
<td>1238</td>
<td>97</td>
<td>8 %</td>
</tr>
<tr>
<td>False accounting</td>
<td>133</td>
<td>9</td>
<td>7 %</td>
</tr>
<tr>
<td>Fraud recovery</td>
<td>368</td>
<td>26</td>
<td>7 %</td>
</tr>
</tbody>
</table>
### Table 4 (continued)

<table>
<thead>
<tr>
<th>Action Fraud category/sub-categories</th>
<th>Total</th>
<th>Cyber-involvement</th>
<th>% of Cyber-involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time shares and holiday club fraud</td>
<td>219</td>
<td>15</td>
<td>7 %</td>
</tr>
<tr>
<td>Application fraud (excluding mortgages)</td>
<td>6350</td>
<td>428</td>
<td>7 %</td>
</tr>
<tr>
<td>Retail fraud</td>
<td>1660</td>
<td>109</td>
<td>7 %</td>
</tr>
<tr>
<td>Fraud by abuse of position</td>
<td>500</td>
<td>29</td>
<td>6 %</td>
</tr>
<tr>
<td>Pension liberation fraud</td>
<td>230</td>
<td>12</td>
<td>5 %</td>
</tr>
<tr>
<td>Telecom industry fraud (misuse of contracts)</td>
<td>3194</td>
<td>119</td>
<td>4 %</td>
</tr>
<tr>
<td>Corporate employee fraud</td>
<td>451</td>
<td>12</td>
<td>3 %</td>
</tr>
<tr>
<td>Computer software service fraud</td>
<td>7813</td>
<td>167</td>
<td>2 %</td>
</tr>
<tr>
<td>Department of Work and Pensions (DWP) fraud</td>
<td>9</td>
<td>0</td>
<td>0 %</td>
</tr>
<tr>
<td>Passport application fraud</td>
<td>1</td>
<td>0</td>
<td>0 %</td>
</tr>
</tbody>
</table>

### Table 5 Median amounts given to fraudster by victim

<table>
<thead>
<tr>
<th>Fraud type</th>
<th>Estimated loss to fraudsters per victim</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pension fraud</td>
<td>£38,974</td>
</tr>
<tr>
<td>Business trading fraud</td>
<td>£28,609</td>
</tr>
<tr>
<td>Financial investments</td>
<td>£21,534</td>
</tr>
<tr>
<td>Bankruptcy and insolvency</td>
<td>£20,000</td>
</tr>
<tr>
<td>Fraudulent applications for grants from government-funded organisations</td>
<td>£11,500</td>
</tr>
<tr>
<td>Fraud by abuse of position of trust</td>
<td>£8100</td>
</tr>
<tr>
<td>Corporate fraud</td>
<td>£3869</td>
</tr>
<tr>
<td>Department of Work and Pensions(DWP) Fraud</td>
<td>£3298</td>
</tr>
<tr>
<td>False accounting</td>
<td>£2000</td>
</tr>
<tr>
<td>Other regulatory fraud</td>
<td>£2000</td>
</tr>
<tr>
<td>Banking and credit industry fraud</td>
<td>£1721</td>
</tr>
<tr>
<td>Insurance fraud</td>
<td>£1084</td>
</tr>
<tr>
<td>Advance fee payments</td>
<td>£784</td>
</tr>
<tr>
<td>Computer misuse crime</td>
<td>£536</td>
</tr>
<tr>
<td>Fraud by failing to disclose information</td>
<td>£440</td>
</tr>
<tr>
<td>None of the above</td>
<td>£420</td>
</tr>
<tr>
<td>All charity fraud</td>
<td>£390</td>
</tr>
<tr>
<td>HM revenue &amp; customs fraud (HMRC)</td>
<td>£281</td>
</tr>
<tr>
<td>Non-investment fraud</td>
<td>£274</td>
</tr>
<tr>
<td>Telecom industry fraud (misuse of contracts)</td>
<td>£112</td>
</tr>
</tbody>
</table>

*a The table illustrates the amounts lost to fraudsters per victim. It is estimated by using the median rather than the average because the averages are skewed by large standard deviations, and often estimations of loss. The Advance fee frauds, for example, are numerous and yield relatively small amounts to fraudsters. The data field is skewed because of some large entries, so, to correct for these, the median has been used to demonstrate the difference.*
to prioritise action (in combination with judgments of how feasible a case will be to take forward to criminal justice). This analysis is presented in Table 6. It shows that the types of fraud with the most impact on the ‘victims’ are: ‘pyramid or Ponzi offences’, followed by ‘dishonestly retaining a wrongful credit’, ‘fraud by abuse of position of trust’ and ‘pension frauds’. By comparison, offline retail fraud has the lowest impact on victims (perhaps because it is likely to be reimbursed via payment card firms). Again the degree of cyber-involvement associated with each type of offence, is highly variable, although cyberfrauds against individuals registers as the most significant in terms of harm.

Notwithstanding the limitations from identification and reporting, the data do point to where the biggest threat from cyberfraud lies (and thus one of the grounds for deciding if this should be one of the main foci of any cyber-related law enforcement response). On the other hand, those categories reflecting the biggest losses – such as pension, business trading and financial investment frauds - are areas where cyber-enablement or cyber-dependency was not an obvious significant factor. Those offences with significant cyber-involvement seem to vary in both number of cases, average loss and likelihood of realistic levels of recovery (where such data is available), as shown in Table 7. The data also show that some of the financial loss of frauds is unlikely to be recovered for the victims (though the number of cases where recovery is known is a small percentage of the total, and the true position is likely to be much worse).

Table 8, conversely, shows that those areas where the greater (mean or median) amounts are likely to be recovered are in the business or public sectors (such as DWP, HMRC, business trading fraud or false accounting) where cyber-involvement is low (the highest level of cyber-involved first contact method was less than 16 %).

Overall the data provide an evidential basis for understanding which frauds have the greater and lesser levels of cyber-involvement, to illuminate some considerations – and challenges – for developing any effective risk-based responses by law enforcement.

**Table 6** Fraud impact levels by self-assessed severity

<table>
<thead>
<tr>
<th>Fraud type</th>
<th>% of severe</th>
<th>Harm factor</th>
<th>% Cyber-involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pyramid or Ponzi Schemes</td>
<td>74 %</td>
<td>2.87</td>
<td>24 %</td>
</tr>
<tr>
<td>Dishonestly retaining a wrongful credit</td>
<td>73 %</td>
<td>2.73</td>
<td>11 %</td>
</tr>
<tr>
<td>Other financial investment</td>
<td>70 %</td>
<td>2.77</td>
<td>17 %</td>
</tr>
<tr>
<td>Fraud by abuse of position of trust</td>
<td>70 %</td>
<td>2.76</td>
<td>6 %</td>
</tr>
<tr>
<td>Rental fraud</td>
<td>68 %</td>
<td>2.70</td>
<td>74 %</td>
</tr>
<tr>
<td>Pension fraud committed on pensions</td>
<td>67 %</td>
<td>2.80</td>
<td>8 %</td>
</tr>
<tr>
<td>Lender loan fraud</td>
<td>66 %</td>
<td>2.68</td>
<td>17 %</td>
</tr>
<tr>
<td>Dating/romance scam</td>
<td>64 %</td>
<td>2.65</td>
<td>88 %</td>
</tr>
<tr>
<td>Other regulatory fraud</td>
<td>62 %</td>
<td>2.67</td>
<td>31 %</td>
</tr>
<tr>
<td>Bankruptcy and insolvency</td>
<td>60 %</td>
<td>2.80</td>
<td>17 %</td>
</tr>
</tbody>
</table>
The implications for an effective risk-based response: what do the data tell us?

The data provide only a ‘snapshot’ insight into cyberfraud, showing that ICT plays a substantial but far from exclusive role in criminal fraud. Before commenting further, we would note two negative or unresolved issues that inform the imperfect nature of the picture the data presents.

First, the data are not completely accurate. The cyber component of reported fraud is ill-represented as a standalone data field. Hard to capture (even for the victim) is when the fraud involves different types of networked technology, such as VOIP through the phone system, enabling offenders to engage cheaply and less identifiably than with traditional technologies with victims online. While cyber-enabled or cyber-dependent economic crime appears to be just over a quarter (27%) of Action Fraud reports, other

Table 7  Estimated median amounts lost to, and recovered from, the fraudster by highest levels of cyber-involvement

<table>
<thead>
<tr>
<th>Fraud type (sub-categories)</th>
<th>% of Cyber-involvement</th>
<th>Estimated median loss per victim (£)</th>
<th>Estimated median recovery per victim</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dating/romance scam</td>
<td>88%</td>
<td>£2595 ($n = 528)</td>
<td>£1700 ($n = 27)</td>
</tr>
<tr>
<td>Online shopping and auctions</td>
<td>86%</td>
<td>£210 ($n = 9329)</td>
<td>£160 ($n = 483)</td>
</tr>
<tr>
<td>Counterfeiting cashiers’ cheques</td>
<td>77%</td>
<td>Not known</td>
<td>£305 ($n = 36)</td>
</tr>
<tr>
<td>Rental fraud</td>
<td>74%</td>
<td>£980 ($n = 603)</td>
<td>£700 ($n = 28)</td>
</tr>
<tr>
<td>Ticket fraud</td>
<td>72%</td>
<td>£450 ($n = 897)</td>
<td>£528 ($n = 32)</td>
</tr>
<tr>
<td>Computer virus/malware/spyware</td>
<td>71%</td>
<td>£100 ($n = 191)</td>
<td>£132 ($n = 48)</td>
</tr>
<tr>
<td>Denial of service attack</td>
<td>55%</td>
<td>£605 ($n = 6)</td>
<td>£6 ($n = 1)</td>
</tr>
<tr>
<td>Mandate fraud</td>
<td>54%</td>
<td>£9820 ($n = 682)</td>
<td>£3845 ($n = 32)</td>
</tr>
</tbody>
</table>

a The number of cases may differ because: a) the recoveries may be from a different time period to the losses; b) there are fewer recoveries than losses because i) there are simply fewer recoveries ii) recoveries from any given set of losses may arise in subsequent time periods iii) there may be inaccuracies in the reporting process (e.g. the losses may be overestimated, or the person who lost the money may not know that it was recovered, say by someone else, such as a bank)

Table 8  Average amounts (median and mean) recovered from fraudsters

<table>
<thead>
<tr>
<th>Fraud type</th>
<th>Amount recovered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial investments</td>
<td>£7107</td>
</tr>
<tr>
<td>Banking and credit industry fraud</td>
<td>£1621</td>
</tr>
<tr>
<td>Corporate fraud</td>
<td>£988</td>
</tr>
<tr>
<td>Pension fraud</td>
<td>£24,244</td>
</tr>
<tr>
<td>HM Revenue &amp; Customs Fraud (HMRC)</td>
<td>£40,141</td>
</tr>
<tr>
<td>Fraud by abuse of position of trust</td>
<td>£1629</td>
</tr>
</tbody>
</table>

The data provide only a ‘snapshot’ insight into cyberfraud, showing that ICT plays a substantial but far from exclusive role in criminal fraud. Before commenting further, we would note two negative or unresolved issues that inform the imperfect nature of the picture the data presents.

First, the data are not completely accurate. The cyber component of reported fraud is ill-represented as a standalone data field. Hard to capture (even for the victim) is when the fraud involves different types of networked technology, such as VOIP through the phone system, enabling offenders to engage cheaply and less identifiably than with traditional technologies with victims online. While cyber-enabled or cyber-dependent economic crime appears to be just over a quarter (27%) of Action Fraud reports, other
indications suggest that cyber-assisted crime is around 60%. Furthermore, it is mistaken to see crimes in a binary way as either online or offline because many start online, until a victim is hooked; then the fraud may go offline. Other crimes stay online all of the time – at least prior to cashing out the proceeds - for example, many dating/romance scams and some other advance fee frauds, and most computer misuse crimes.

The second issue is the lack of information on perpetrator profiles and their organisation or interaction, information sources and approaches. Victims seldom know to what extent ‘organised crime’ is involved or whether those involved are highly computer literate or rely on crimeware-as-a-service where cybercriminals access online specialists to supply to them the means, such as malicious software, supporting infrastructure, stolen personal and financial data. The data especially do not allow easy identification of how far the same groups or individuals operate different frauds, how far they specialise, whether (or how) they share approaches, software or lists of potential victims (repeat victimisation is a noteworthy feature of cyberfraud), how they network, organise or cooperate.

Despite respondents’ beliefs at the time of reporting that 97% of ‘their’ offenders were in the UK, we also know that the geographic location of the perpetrators, or the locations for different aspects of the crime, including servers, is very difficult to identify – with all the attendant difficulties of investigation and prosecution where there is an overseas dimension. In other words, the crime scenes, as well as the likelihood of access to documents, witnesses and equipment, are less clear than the data make them appear to be.

On the other hand, the Action Fraud data do reveal a complex and nuanced picture of cyberfraud with significant but specific types of cyber-dependant, cyber-enabled and cyber-assisted crimes, information on losses and number of incidents, differentiated patterns of cyber-involvement and the impact on victims. We can argue that cyber-enabled fraud reflects much greater financial losses than cyber-dependant crimes, whose losses are more likely to be incurred through payment for business disruption and recovery. In particular we would note in terms of responses:

- There is a high level of cyber involvement in reported cases of fraud, but there is no established pattern of what crimes are cyber-involved, or who carries them out;
- Cyber-involvement is an elastic term, given its role among a number of other media in initiating and perpetrating frauds;
- Financial losses can be substantial by case, by crime, but there are variations – not all cyberfraud results in significant losses and not all frauds involve ICT (except perhaps in the trivial sense that financial transfers usually are electronic, whatever form they take);
- Even in those industries with well-established prevention and protection approaches, such as financial services, the level of reported cyberfraud and cybercrime remains high, though much is prevented;
- The level of loss recovery from cyberfrauds is relatively low (as it also is from other crimes: see [17]).

The key point from the data is that the main perception or fear of cybercrime relates to denial of access, disruption and loss of data and identifiers (see [12]) but, in practice, few of these result in actual immediate and direct financial loss to victims. There is a
substantial level of high-volume, often low-value, cyberfraud with varying degrees of harm, in which the cyber component varies by crime. This heterogeneity can and should influence law enforcement responses, but not in a simple way either for prevention or for offender pursuit.

The implications for an effective response: what are the main issues for any law enforcement response?

From the victim perspective, the data do address some significant policy- and law enforcement-related issues within the volume-value-category-cyber matrix: the majority of cyberfrauds are high-volume, low value with low levels of recovery, usually targeted at individuals. Thus we need to be concerned not merely whether or not a differentiated response is required at national and local levels, but also whether such a response requires a reactive investigative response and/or a technical-led investigative capability; whether the emphasis should be on awareness and education and how should any response balance volume, loss, harm, perpetrator or deterrence as the main drivers of any response. Such a response should also take into account the empirically tested effectiveness of individual and national level reduction mechanisms [2].

Second, and not unique to cyberfrauds, any response has to take account of a landscape that changes dramatically as networked technologies transform the way that fraud could be organised, as cybercrime has become more professional, harder to identify and/or recognise, and provides anonymity for offenders, at least under normal conditions, without significant forensic investigation efforts that are highly limited in absolute availability and cost. An emerging and dynamic cybercrime threat landscape that challenges policing is the human-centred interactive ecosystem of the Social Web where the threats posed by cybercrime frequently elude more traditional approaches to policing. Activity conducted via the Social Web represents a new frontier for national and international security and crime fighting, yet such interactive spaces remain largely unregulated. Given the scale, international reach and open nature of the Social Web, the police struggle to meet an expectation of protection from the public, due not just to resources and skills but to a perceived lack of actionable intelligence on emerging cyber threats. As technologies become cheaper and more widely available, the increase in global internet penetration, new users, activities and products will be incorporated into what is now a global online community, growing the pool of both potential victims and criminal actors. Easier access means a greater proportion of users than previously may be unfamiliar with technologies, making them ‘easy targets’ both as intermediaries for (e.g. botnets, money mules) and as victims of fraud.

Third, the Action Fraud reports and other data from CIFAS and FFAUK suggest that cyberfrauds have been rising, though the lack of comparable data for previous years makes this a matter of very plausible interpretation rather than demonstrable fact (see Levi, this volume). Given the rise in the number of Internet-enabled devices and the proportion of the population who are connected, it would be a surprise if this were not

---

7 Examples of the Social Web include online interactive mainstream media, interactive blogs, and the suite of technologies often referred to as social media.
so. Given a large number of people around the world with the motivation to defraud and so many situational opportunities outside their domestic jurisdictions that the internet now provides, it may be impressive (but not reassuring) that the reported cyberfraud rate is not higher. Strategic planners need to consider what it would take to produce a much higher (or lower) cyberfraud rate.

The data also indicate that there are significant variations in the impact of cyberfraud by crime category and even within the latter, there are non-trivial variations in the level of cyber involvement in the crime, in the types of victims (whether businesses or individuals), the interplay between cyber involvement and other communication modes for the commission of the crime, and the losses associated with the crime. Such variations have implications for effective risk-based responses.

The implications for an effective response: what should be the main considerations for policy?

First, as it is the sovereign responsibility of the state to protect its citizens, including its critical national infrastructure, financial services, key commercial intellectual property and government secrets, against cybercriminals, including other national governments, it is a reasonable demand to require government to provide the necessary state response, requiring the engagement of the intelligence agencies, strong and effective intra- and inter-country collaborative, information-sharing and support networks. Certainly it would be expected that any national government develops a strategy that seeks to address cybercrime and to identify those government and other agencies to whom specific roles and responsibilities, as well as resources, could be devolved.

Second, given the trends and approaches to both policing and to fraud, as noted above, there is likely to be a clear limit to the reliance on an open-ended law enforcement response, and to a reliance solely on law enforcement to respond, given the median amounts involved, the investigative and evidential accessibility, the low likely recovery of the proceeds of cyberfraud, and the problematic nature of both crime scene and geographic location of perpetrators. Clearly policing cyberfraud involves a multiplicity of national and transnational actors intervening both before and after the criminal activity: but it is not clear how far law enforcement, given its competing agendas and resources, can investigate cyberfraud that has – or may have - international dimensions which are not readily penetrable on a routine basis.

Third, there may be a symbolic need for law enforcement to show particular criminal networks and individuals that involvement in crime has its costs, even if – as has been shown in the rapid revival of alternative drug and identity data cryptomarkets following take downs such as DarkMarket, Silk Road and Onymous (see Décary-Hétu and Giommoni, and Dupont, this volume) – the impact on crime and precursor availability is modest. Target audiences may include not just the immediate offenders but others at home and abroad, and also potential perpetrators, victims and potential victims who may need reassurance and/or a continuing message of intent. Similarly, the technical knowledge from investigations and inter-country cooperation would be essential inputs into organisations in both public and private sectors to ensure their in-house capacity is informed with credible awareness and alert campaigns. If part of the police reaction is to be intelligence -led and proactive, how is this to be achieved? What kinds of fresh
and existing sources can be deployed to get a better and quicker picture of offending and offender networking than exist at the present?

Fourth, we are persuaded from the Action Fraud data that relatively little of the reported cyberfraud lends itself to a traditional reactive law enforcement response, though it may be susceptible to specifically targeted significant awareness and prevention campaigns (‘Protect’ and ‘Prepare’ in the jargon of the Home Office) that aim to encourage new and bolster existing individual level security behaviours, some of which have been shown to be effective in reducing cybercriminal victimisation [2]. Even once messages are disseminated, on radio, television, the press, and via friends and families, however, there are always some that do not follow the advice or who wrongly interpret the message and engage in economically damaging avoidance behaviours, and consideration may have to be given to automated security with opt-out rather than opt-in requirements (for example, for on-line banking), especially if insecurity can cause problems for others, like botnets.

Here we suggest also that further research, like that of Williams [2] on the effectiveness of individual level security behaviours, and behavioural studies on mechanisms of security adoption, be done on national longitudinal datasets where they exist. Such research would help identify what needs to be done to enable and nudge such people to take action to protect themselves and make better informed judgments, whilst allowing them to continue to enjoy the benefits of the internet. Certainly the imperfect information on the nature, motivation and geographic location of the perpetrator, as well as the limited likelihood of any law enforcement intervention would require a ‘nudge’ to financial and other services to be more proactive in requiring the use of mandated software, if only to encourage more security awareness and less self-determination among businesses and the public, particularly for those who do not have a common understanding of what to do to protect themselves, and why.

There is scope for a more dynamic, structured and response-focused approach to guidance, warnings and awareness-raising, including the identification of and support for organisations and media sources that have an established engagement with individuals who may thus be more predisposed to listen. Similarly, there is a role for law enforcement or other approved bodies to set up educational ‘mock operations’ to warn users who respond to fraudulent offers of different kinds (created by the authorities) that they could have become victims of fraud, via on-screen ‘pop ups’ (such tactics could also be used on criminal marketplaces as warnings to those seeking illicit products or co-offenders on the web.) This may have particular resonance for repeat victims.

An effective response: what should be the overarching themes?

Overall, we are not in a position to offer a fully-evidenced effective risk-based strategy to address risk and threats where there is no clear answer from the data, but we would argue that the Anglo-Welsh case study provides a basis for continuing dialogue on these important social and economic issues, which touch an ever-increasing proportion of the population in the UK and elsewhere.

If we are asked to consider that would be a general optimal law enforcement response in the light of these data, and bearing in mind the problems that law
enforcement, organisations, and governments will continue to face in cost to pay-off questions vis-à-vis cybercrimes, we would argue that this must range from the internet server and services providers actively developing means to promote secure use and reduce the risk of threat of economic loss, to using transnational criminal justice to render the most damaging cybercrimes unprofitable, and to engaging users and customers in a proactive awareness of prevention and protection. Further, any role in cyberfraud reduction shows the need for clarity in tasking and in the messaging from strategic, operational and symbolic police actions. Assessing the cost, impact or added-value of investigations or prosecutions, disruption and asset recovery on domestic and foreign offenders remains in its infancy (see Dupont and see Décary-Hétu & Giommoni, this issue; see also [18, 19]): but it needs very careful consideration for each case, particularly in terms of cross-border intelligence and cooperation arrangements. In addition, and in line with contemporary approaches to partnership/’plural’ policing and engagement with stakeholders and communities of interest, attention needs to be given to the roles and responsibilities of the network of relevant agencies and industries (the UK Information Assurance community, including Cyber-security Information Sharing Partnership initiatives -https://www.cert.gov.uk/cisp/) and to a realistic assessment of what they may be better placed to provide, or able to offer in the way of complementary support [8]. This is a dynamic process, and the negotiation of agreements and resourcing are a necessary but not sufficient condition of actual cooperation.

There is an important self-interest not only in organisations taking their own initiatives to address cybercrime but also in coordination and cooperation between organisations, where the law enforcement role will be primarily one of disruption and occasional deterrence, as well as providing guidance and information on emerging risks and threats, issues particularly true of small to medium enterprises (SMEs). Larger organisations often have dedicated ICT departments and are better informed of the risks and threats. They are also likely to be able to afford the appropriate resourcing responses. For them, the issue is less of awareness and education, or even having access to law enforcement resources to investigate and prosecute fraud, than access to specialist guidance on threat and risk profiles and types to design and deploy responses, leaving law enforcement to identify and take action against the identifiable groups who initiate the more significant or recurring cyber-attacks against them. For SMEs, dedicated awareness and educative responses are required [8]. A combination of experience to increase perceptions of risks and having mitigations/solutions in place would likely help overcome the resource, expertise and scepticism barrier for the majority. It is important here to consider the need for ‘knock-on’ effects, such as through the supply chain, which can generate systemic weaknesses if not addressed. It may also be important to supplement such responses with specialist guidance and advice on a planned basis.

Of much more concern is addressing the same challenges at the level of the individual victims where, as the Action Fraud data suggests, the majority of cyberfrauds by number, though not by value, take place. Any strategy for policing cyberfraud needs to have a significant educative component that is intelligible (a) to victims and intended victims and (b) to those in a position to monitor behaviour and provide relevant advice. Such an approach also has to recognise and reflect the specific characteristics of the crime itself. People have to have a common understanding of what
to do to protect themselves, and why, know what to do and to actually carry out these measures and review them over time. Cyber-fraud prevention is not a one-time effort, and both online and offline social engineering seeks to move potential victims away from the protections they might know about in the abstract to their informed use in practice.

There is scope for a more dynamic, structured and response-focused approach to guidance, warnings and awareness-raising, and the police can play a collaborative role in arrangements to provide that advice before and after individuals become victims. For public reassurance and for deterrence/incapacitation, some police action is needed and more up-skilling for existing officers – or employing specialist civilian staff - is necessary. Some 5000 police have been given a modest amount of training via the College of Policing, and this is a beginning. Our suggested next steps for this include the need for better, early education of risk management and a focus on helping vulnerable citizens to appreciate and manage the risks of both online and offline fraud, and this may be better done via peers and the third sector than by the police and websites alone, however user-friendly.

Conclusion

The routinisation and pervasiveness of internet use has made certain types of internet-based crimes for economic gain possible (cyber-dependant economic crimes), and has facilitated immensely the scale of others (cyber-enabled and cyber-assisted economic crimes) by reducing the cost and effort of reaching out to potential victims. Cyberspace content is constantly evolving, for an extensive range of functions, services and products, while also providing platforms for aggregation and innovation, in the perpetration of cyberfraud. Cyberspace has multiple criminal actors living in many jurisdictions whose typologies and methods of organisation and operation do not lend themselves easily to existing definitions and understanding, e.g. in terms of ‘hotspots’ analysis.

Cyberspace is developing its own criminal marketplaces and financial arrangements, some of which require specialist awareness and access to address. The perpetration of cyberfraud outstrips current preventative and other measures for control protection and has increased the difficulties of identifying, investigating and prosecuting offenders as much as it has increased vulnerabilities among businesses, governments and to individuals (including the general public). There is widespread agreement that policing in the UK and also around the world has fallen behind the curve of evolving patterns of crime, especially cyberfrauds and the cyber-forensic aspects of police investigations. The latter is expensive and time-consuming, even disregarding the enormous forensic resources for child sexual exploitation online.

Given the very differentiated and nuanced nature of cyberfraud, however, it is clear that any response, including that of law enforcement, must be a collective and strategic approach with the intention of: Increasing the effort the offender must make to carry out the crime; increasing the risks the offender must face in completing the crime, including cashing out the proceeds; reducing the rewards or benefits the offender expects to obtain from the crime; removing excuses that offenders may use to rationalise or justify their actions; reducing incentives, opportunities and access to expertise that may tempt
or incite offenders into criminal acts; increasing the awareness of potential victims of the need for prevention and understanding of risk; increasing the roles and responsibilities of internet providers, and organisations who provide services through the internet, in building in security and building in buy-in from users, customers, etc.; and balancing guidance, reassurance and deterrence in a way that appears to recognise and respond, cost-effectively, to the evidence base of the risk and the threat, an evolving process.

Cyberfraud harms the interests of almost all licit business, government and individuals, though not equally. The need for a law enforcement response is unquestionable in principle but is hedged by a plethora of issues and limitations in practice, and is not feasible for a large proportion of frauds. In this context, we would argue that any law enforcement response must begin by being strategic: which other bodies should be involved to do what; what should be the specific roles and responsibilities of the police and where ‘problem ownership’ should lie in terms of cybercrime and cyberfraud; what we (and sub-sets of ‘we’) are prepared to pay for (in money and effort) for greater cybersecurity; and, how that security is going to be organised for and/or by the huge numbers of businesses and people that are actually and potentially affected, that will broaden further with the risks posed by the Internet of Things. We argue that the UK case study provides some grounded data on which to take these issues forward, although we would also caution that many initiatives are emerging rather than comprehensive and well-established in a developing dynamic commercial environment. Whatever measures are adopted, it is unlikely that they will be simple harm reduction processes (like wearing seat belts) but will need to evolve with both private and public sector governance.

References


