Measuring the Cost of Cybercrime

Ross Anderson [1] Chris Barton [2] Rainer Böhme [3] Richard Clayton [4]
Michel J.G. van Eeten [5] Michael Levi [6] Tyler Moore [7] Stefan Savage [8]

Abstract

In this paper we present what we believe to be the first systematic study of the costs of cybercrime. It was prepared in response to a request from the UK Ministry of Defence following scepticism that previous studies had hyped the problem. For each of the main categories of cybercrime we 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. We distinguish 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 find 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. However, the indirect costs and defence costs are much higher for transitional and new crimes. For the former they may be roughly comparable to what the criminals earn, while for the latter they may be an order of magnitude more. As a striking example, the botnet behind a third of the spam sent in 2010 earned its owners around US$2.7m, while worldwide expenditures on spam prevention probably exceeded a billion dollars. We are extremely inefficient at fighting cybercrime; or to put it another way, cyber-crooks are like terrorists or metal thieves in that their activities impose disproportionate costs on society. Some of the reasons for this are well-known: cybercrimes are global and have strong externalities, while traditional crimes such as burglary and car theft are local, and the associated equilibria have emerged after many years of optimisation. As for the more direct question of what should be done, our figures suggest that we should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response – that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail.

[1]Computer Laboratory, University of Cambridge, JJ Thomson Ave, Cambridge, CB3 0FD, UK. ross.anderson@cl.cam.ac.uk

[2]UK. chris@vnworks.net

[3]University of Münster, Department of Information Systems, Leonardo-Campus 3, 48149 Münster, Germany. rainer.boehme@wi.uni-muenster.de

[4]Computer Laboratory, University of Cambridge, JJ Thomson Ave, Cambridge, CB3 0FD, UK. richard.clayton@cl.cam.ac.uk

[5]Faculty of Technology, Policy and Management, Delft University of Technology, Jaffalaan 5, 2628 BX, Delft, Netherlands. M.J.G.vanEeten@tudelft.nl

[6]School of Social Sciences, Cardiff University, Cardiff, CF10 3XQ, UK. levi@cf.ac.uk

[7]Department of Computer Science and Engineering, Southern Methodist University, Dallas, TX 75275, USA. tylerm@smu.edu

[8]Department of Computer Science and Engineering, University of California, San Diego, CA 92093, USA. savage@cs.ucsd.edu

1 Introduction

As countries scramble to invest in information security, governments want to know how large that investment should be, and what the money should be spent on. This creates a demand among rational policy-makers for accurate statistics of online/electronic crime and abuse. However, many of the existing surveys are carried out by organisations (such as antivirus software vendors or police agencies) with a particular view of the world and often a specific agenda. This paper therefore sets out to collate what is known, and what is not, as of the beginning of 2012.

It builds on a report written by four of us in 2008 for the European Network and Information Security Agency, 'Security Economics and the Single Market' [2]. There we analysed the statistics available at the time, their shortcomings, and the ways in which they could lead to incorrect policy decisions.

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 purchase antivirus software. This is part of a much wider problem of attributing risks to patterns of offending.

There are over 100 different sources of data on cybercrime, yet the available statistics are still insufficient and fragmented; they suffer from under- and over-reporting, depending on who collected them, and the errors may be both intentional (e.g., vendors and security agencies playing up threats) and unintentional (e.g., response effects or sampling bias). The more prominent sources include surveys (from Eurostat, CSI and consultancies); security breach disclosure reports; direct observations of attack trends (e.g., from Symantec, McAfee and Microsoft); and reports by trade bodies (from banking trade associations, or the Anti-Phishing Working Group). We compared and analysed the CSI, Eurostat and Symantec statistics in the aforementioned ENISA report [2].

The proximate motivation for this paper was a request from the Chief Scientist at the UK Ministry of Defence, Sir Mark Welland, for an update on the analysis we produced in the 2008 report. This was driven in turn by the publication in February 2011 of a report [10] commissioned by the UK Cabinet Office from Detica (part of BAE plc) which estimated cybercrime's annual cost to the UK to be £27bn (about 1.8% of GDP). That report was greeted with widespread scepticism and seen as an attempt to talk up the threat; it estimated Britain's cybercrime losses as £3bn by citizens, £3bn by the government and a whopping £21bn by companies. These corporate losses were claimed to come from IP theft (business secrets, not copied music and films) and espionage, but were widely disbelieved both by experts and in the press. The Ministry of Defence asked us to set out what figures are known, what can reasonably be estimated and what can only be guessed.

We begin by setting out a framework for analysing the costs of cybercrime in Section 2, differentiating cybercrimes from physical ones and decomposing cost categories. Next, in Section 3 we review available information on costs for all substantial categories of cybercrime. We discuss the costs of the common infrastructure facilitating many types of cybercrime in Section 4, and we present the costs together in summary form in Section 5 before concluding in Section 6.

2 A Framework for Analysing the Costs of Cybercrime

Even before computers started to make things more complicated, it was already hard to define and measure white-collar crimes. While it's clearly a crime to set up a fly-by-night mail-order firm, collect payments and ship no goods, the situation is less clear when goods are mis-described or defective. Periodic scandals (McKesson & Robbins in 1938, IOS and Equity Funding in 1973, Enron in 2001, the banking crisis in 2008) raise questions about the boundary between business and crime, leading to changes in definitions as well as regulations. These shifts are associated with changes in social attitudes and political discourse; for a discussion see [38, 37].

While tying down fraud was hard enough a decade ago, globalisation and technology are making the problem harder still today. Many corporations are transnational, as are many cybercrimes. If a Chinese gang steals secrets from BAE, is this a UK crime as BAE has its primary stock-market listing in London, or a US one as it does more business there? Furthermore, while there are some online and electronic crimes for which we have UK figures (such as card fraud) there are others for which we have only global figures (such as the incomes of gangs selling fake pharmaceuticals or operating botnets). In the circumstances the sensible way forward is to estimate global figures. We will work from the fact that the UK accounts for about 5% of world GDP to scale our national estimates up or down as appropriate. Where there is reason to believe that the UK figures are out of line with other countries, we will say so and make an appropriate allowance.

2.1 Differentiating cybercrime from other crime

In May 2007 the European Commission issued a Communication "towards a general policy on the fight against cyber crime", noting that there was not even an agreed definition of cybercrime [12]. It proposed a threefold definition:

1. traditional forms of crime such as fraud or forgery, though committed over electronic communication networks and information systems;
2. the publication of illegal content over electronic media (e.g., child sexual abuse material or incitement to racial hatred);
3. crimes unique to electronic networks, e.g., attacks against information systems, denial of service and hacking.

We propose to follow this definition here, despite the fact that the boundary between traditional crime and cybercrime remains fluid. Advances in information technology are moving many social and economic interactions from the physical world to cyberspace, so a moving boundary between cyber and physical is inescapable. For example, the UK will move all claims for welfare payments online in 2013, and most claims are made that way already; welfare fraud is 0.8% of the £152bn expenditure of the Department of Work and Pensions, or a tad over £1.2bn. Income tax fraud (evasion as opposed to avoidance) adds about a further £3bn. These sums dwarf the amounts stolen by 419 fraudsters or even carders. What is important is to have a yardstick with which to measure changes. For that reason, we have to decompose fraud figures into different categories.

We must also not lose sight of the big picture. The reduced transaction costs and economies of scale brought by the Internet have unleashed substantial productivity gains [3]. We may hope

that the overall costs of crime will go down, in the sense that the value of the electronic versions of old-fashioned crimes will decrease by more than the value of new crimes made possible by new technology. Nevertheless, we should bear in mind that even if the costs of crime go up, there may still be a substantial net gain for society.

2.2 Decomposing the cost

As for measuring costs, the Detica report considered four categories:

1. costs in anticipation of cybercrime, such as antivirus software, insurance and compliance;
2. costs as a consequence of cybercrime, such as direct losses and indirect costs such as weakened competitiveness as a result of intellectual property compromise;
3. costs in response to cybercrime, such as compensation payments to victims and fines paid to regulatory bodies;
4. indirect costs such as reputational damage to firms, loss of confidence in cyber transactions by individuals and businesses, reduced public-sector revenues and the growth of the underground economy.

We will not use this methodology as it stands, as the second heading includes both direct and indirect costs of which the former might at least in principle be measured accurately while the latter are harder to assess. The third item we view as being composed entirely of direct costs: if a bank designs an insecure website and has to pay compensation to customers whose accounts are debited without their mandate, these are clearly direct costs. We therefore use a more straightforward approach, in which we simply split direct costs from indirect costs. We will also have some things to say about the costs of security (though these cannot always be allocated to specific types of crime) and about the social and opportunity costs of reduced trust in online transactions.

Where possible we will decompose the costs of crime still further. Just as a thief who steals the lead from a church roof, or copper wire from a railway signalling system, may earn a handful of cash while doing damage that costs tens of thousands to repair (and disrupts the lives of thousands), so there can also be large asymmetries in costs and revenues.

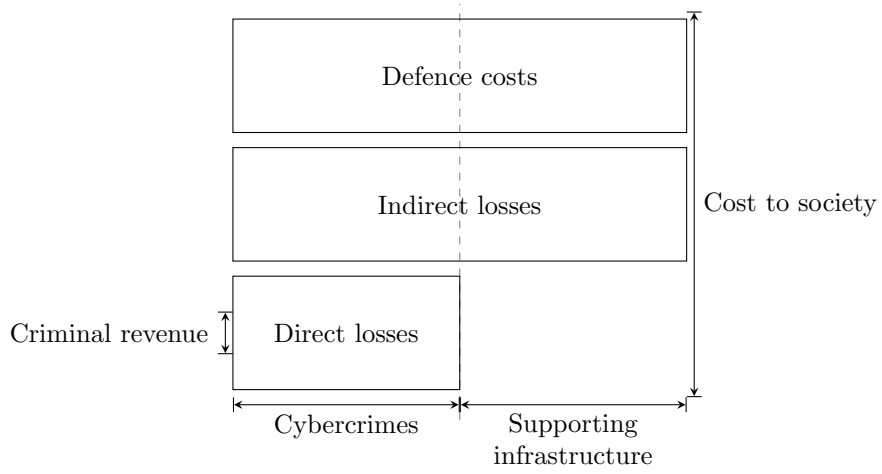
Figure 1 visualizes our framework. We define and discuss its cost categories as follows:

Criminal revenue Criminal revenue is the monetary equivalent of the gross receipts from a crime. We do not include any 'lawful' business expenses of the criminal.[1] For example, an illicit online pharmacy may purchase hosting services from a legitimate provider and pay the market price. This reduces the criminal's profits, but contributes to the gross product of the economy in which the provider is located.

But consider phishing advertised by email spam. The phisherman's criminal revenue is the sum of the money withdrawn from victim accounts. If spamming is also a crime, and is carried out using a botnet (a network of subverted PCs, see Sect. 4.1), then the revenue of the spammer, possibly split with the 'owner' of the botnet, must also be accounted as part of the criminal-revenue contribution to GDP.

[1]The UK Proceeds of Crime Act does not allow an offender's costs to be deducted from the amount he's deemed to owe the state

Figure 1: Framework for analysing the costs of cybercrime



Direct losses Direct loss is the monetary equivalent of losses, damage, or other suffering felt by the victim as a consequence of a cybercrime.

Example: Direct losses include:

- money withdrawn from victim accounts;
- time and effort to reset account credentials (for both banks and consumers);
- distress suffered by victims;
- secondary costs of overdrawn accounts: deferred purchases, inconvenience of not having access to money when needed;
- lost attention and bandwidth caused by spam messages, even if they are not reacted to.

As a practical matter we will generally disregard distress; victims are not generally entitled to sue for it, it is hard to measure, and it is generally worst when exacerbated by secondary victimisation (such as banks disbelieving complaints from victims). Even if we chose to include distress (as has been done in Home Office studies of the costs of violent crime) there is limited data available about the costs of the time spent repairing 'stolen'[2] identities.[3]

Indirect losses Indirect loss is the monetary equivalent of the losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out, no matter whether

[2]Banks may like to describe impersonation as 'identity theft' as it carries with it an implied liability shift – that it wasn't the bank's money that was stolen but the customer's 'identity'. This is controversial; as well as dumping liability it increases the fear of crime. Victimisation studies, such as the BCS and GetSafeOnline, show considerable public anxiety about card fraud and impersonation

[3]The US Identity Theft Resource Center studies the time taken by victims to 'repair' damage caused by 'identity theft'. In 2004, it was more than 300 hours; in 2008, 76 hours; and in 2009, 68 hours [17]. This survey, although interesting, is rather limited in that there were just 203 victims reporting their experiences and they were all assisted by the ITRC, and so might have been reasonably efficient at dealing with their problems.

successful or not and independent of a specific instance of that cybercrime. Indirect costs generally cannot be attributed to individual victims.

Example: Indirect losses include:

- loss of trust in online banking, leading to reduced revenues from electronic transaction fees, and higher costs for maintaining branch staff and cheque clearing facilities;
- missed business opportunity for banks to communicate with their customers by email;
- reduced uptake by citizens of electronic services as a result of lessened trust in online transactions;
- efforts to clean-up PCs infected with the malware for a spam sending botnet.

Observe in Figure 1 that indirect losses is the first category to span both cybercrimes and its supporting infrastructure. The whole idea of distinguishing criminals' profit centres from the common infrastructure being employed in the crimes is to avoid allocating the collateral damage caused by the infrastructure to the actual types of cybercrimes, where they would show up as indirect losses. 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.

Defence costs Defence costs are the monetary equivalent of prevention efforts. They include direct defence costs, i.e., the cost of development, deployment, and maintenance of prevention measures, as well as indirect defence costs, such as inconvenience and opportunity costs caused by the prevention measures.

Example: Defence costs include:

- security products such as spam filters, antivirus, and browser extensions to protect users;
- security services provided to individuals, such as training and awareness measures;
- security services provided to industry, such as website 'take-down' services;
- fraud detection, tracking, and recuperation efforts;
- law enforcement;
- the inconvenience of missing an important message falsely classified as spam.

Defence costs, like indirect losses, are largely independent of individual victims. Often it is even difficult to allocate them to individual types of cybercrime. Defences can target the actual crimes or their supporting infrastructure, and the costs can be incurred in anticipation of or reaction to crimes, the latter being to deter copycats.

Cost to society The cost to society is the sum of direct losses, indirect losses, and defence costs.

2.3 Discussion of the framework

As we shall see, criminal revenue is in practice significantly lower than direct losses and much lower than direct plus indirect losses. In a classical analysis, policy may be guided by looking at direct or indirect losses; a company may invest in protection to the extent that this reduces its direct costs, while a government might consider indirect losses and invest in collective defence efforts (such as policing) so long as every extra unit of defence spending reduces the sum or direct and indirect losses by at least as much.

It is possible to spend too much on defence. The 9/11 Commission estimated that the September 2001 attacks cost no more than $500 000 to carry out [47], but in 2008 it was estimated that the USA had already spent over $3 trillion on defence costs and on the wars in Afghanistan and Iraq [53]. Criminologists examine the widely different expenditure on preventing deaths from terrorism, road traffic accidents, and domestic violence in terms of 'signal crimes' [25] where the symbolic dimensions reach into the general psyche and demand action. One can put a price on this – using 'willingness to pay' models – but there is not a simple cost equation.

Such behavioural theories may not be sufficient to explain all irrational expenditures in the case of cybercrime. For example, it's been reported that the botnet behind a third of all the spam sent in 2010 earned its operators a mere $2.7 million in profit from sales of knockoff pharmaceuticals, while the cost of spam to ISPs and users worldwide is in the billions [33]. Thanks to spam filtering, spam is no longer salient to most citizens in the way that terrorism is.

The misallocation of resources associated with cybercrime results mostly from economic and political factors rather than from behavioural ones. Globalisation means that for much online crime, the perpetrators and victims are in different jurisdictions. This reduces both the motivation and the opportunity for police action. In the case of spam, for example, it's not socially optimal for ISPs to be spending hundreds of millions of dollars on coping with floods of spam; a more rational policy would be to arrest the criminals. Yet the Russian state has not co-operated sufficiently for this to happen. The long-term winners may be firms like Google and Microsoft as people are driven to webmail services with good spam protection.

We will return to this complexity in the conclusions. In the next two sections we collect what is known about the actual costs, and add our own estimates where appropriate. Section 3 iterates through all relevant types of cybercrimes, the cybercriminals' profit centres. Many of these activities rely on a universal infrastructure, based on botnets. These are set up and operated for criminal purposes, and specialized to support cybercrimes, launch attacks, and cover up traces. This infrastructure is a cost centre for cybercriminals, yet the criminals do not pay the full price as the subverted PCs are paid for by their owners. Negative externalities are borne by society in the form of indirect and defence costs. These costs cannot for the most part be attributed to individual crimes and are discussed separately in Section 4.

3 What We Know

Few of the existing measures of cybercrime try to unbundle the different types of crime and categories of cost described above. In the following two sections, we summarize what is known. We also comment on the strength of evidence, and then pull together the numbers below in Section 5. In our summary table we will only record crimes that impose costs in excess of $10m per annum worldwide.

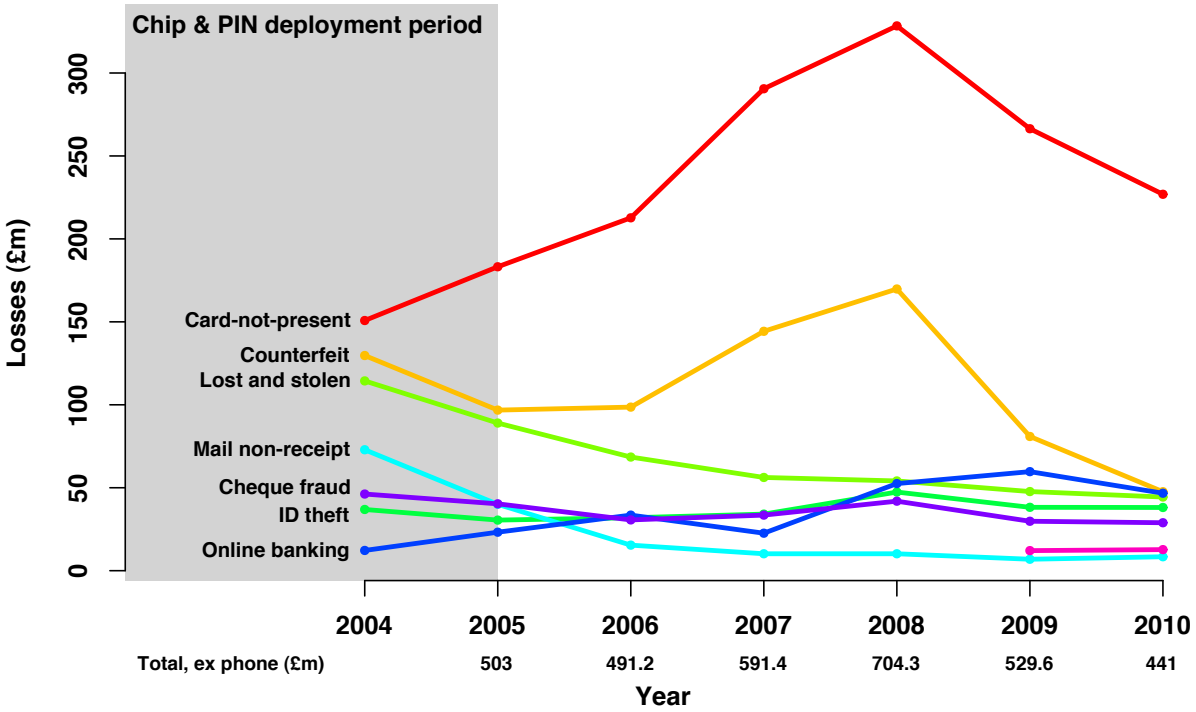


Figure 2: UK card fraud by category during and since the introduction of EMV ('chip and PIN') (Source: UK Payments Administration)

3.1 Online payment card fraud

Bad things that happen on the Internet most commonly have a direct effect on real citizens when a charge they don't agree with appears on their credit card statement or bank statement. The UK Payments Administration, a payment industry trade association, publishes annual reports. Their most recent figure for 2010 puts card-not-present fraud in Internet transactions at £135 million for UK-issued credit and debit cards; the history of their card fraud statistics is set out in Figure 2. The £135 million is a lower bound for the direct costs because even if these are accurate accounts of all the banks' costs and losses, the banks are not the only victims. There is unnoticed and unreported fraud, and there are wrongly denied claims (a hotly contested area). In these cases, the losses stay with the cardholder. Disputed transactions where a PIN was not used are routinely charged back to the merchant, and merchants may wrongly claim that a PIN was used to pass liability back to the bank (and ultimately the cardholder). Moreover, some fraud attempts get recouped; as well as cutting the banks' losses, this may add to the defence costs, while leaving the direct losses with middlemen (who are potentially victims, as in the case of 'money mules'). Overall, there are some grounds for suspicion that some of the drop in reported bank losses since 2008 is not due solely to better fraud prevention but also to more vigorous dumping of liability on merchants and cardholders. We'll return to this later.

Indirect losses are very difficult to quantify. They will have two major components: losses due to lack of confidence by consumers, and business foregone by merchants out of the fear of fraud. A rough proxy for the former is Eurostat's ICT survey, according to which 14% of the UK consumers stated in 2010 that they refrained from buying goods or services online because of security concerns.Yet we must not scale the £27 billion online retail sales (9.5% of total) in the

UK[4] to the 8.7 million of lost online customers, because lost online sales are largely retained as offline sales. The benefits of online over offline sales include reduced consumer search costs and reduced distribution costs, both leading to lower prices as elasticity of demand increases and competition intensifies [40]. Only reduced search costs have a net effect on the economy and may guide estimates of indirect losses – disregarding other possible effects such as wider product differentiation leading to higher prices in the long run [34]. Considering that online merchants or distributors may more often be sited abroad than their offline counterparts, the domestic loss caused by forgone online sales is even lower. This would lead us to estimate the indirect costs of loss of confidence by consumers at perhaps $700m.

As for caution on the part of merchants, there is a regular survey of online merchants carried out by Cybersource, a VISA company that does credit card processing [31]. Merchants reported lost revenues of 1.8% of turnover, mostly to chargebacks, of which 32% were ascribed to fraud; at the same time, merchants rejected 4.3% of orders out of fear of fraud. This is double the figure of 30 basis points that capable online service firms expect to lose to fraud. Then again, Cybersource is trying to sell credit-card fraud prevention services, so perhaps it is not surprising their numbers are at the high end of the plausible range. Suppose that a capable firm might turn down valid orders amounting to 2% of online turnover. A 2009 BCG report assessed the UK's 'digital economy' at £100bn or 7.2% of GDP [28] but of this only half was actual online shopping. So we might rate the indirect losses at 1% of the 'digital economy', or $1.6bn, or a bit more than double what we might infer from Eurostat for the consumers. (We'll gross up the two figures by somewhat less than the usual GDP multiplier of 20 to account for the fact that the UK has relatively weak protection for bank customers compared, for example, with the USA.)

As for defence costs, we will estimate the total for card and bank fraud at the end of Section 3.3, as the terminals used to accept cardholder-present transactions account for the largest single slice of the investment, and perhaps a third of the whole.

3.2 Online banking fraud

Online banking fraud is often conflated with payment card fraud, since both target the financial system and affect banks. However, we distinguish them for several reasons. First, the fraud is perpetrated differently. In online banking fraud, a customer's credentials (e.g., username and password) are obtained by a criminal, who then logs in to the account and initiates transfers to an intermediary who is cooperating with the criminal. Second, the fraud figures are collected separately although, unfortunately, the figures on online banking fraud are less reliable than for card fraud. Third, the parties affected are different: banks and their customers (both consumer and business) suffer online banking fraud, whereas with card fraud consumers, merchants and banks are impacted, and suffer significant administrative costs dealing with disputed transactions.

Online banking fraud is primarily carried out in two ways. In a phishing attack, criminals impersonate bank websites in order to get unsuspecting users to provide their login credentials. Several reports have investigated the revenues available to criminals for phishing. In one study, Moore and Clayton estimated that between 280 000 and 560 000 people gave away their credentials to phishing websites each year [45]. To arrive at a rough estimate of criminal revenue, the authors multiplied this figure by an estimate from Gartner that identity theft costs an average of $572 per victim.[5] Thus, their 2007 estimate was that criminals could earn $320 million per

[4]Source: Office for National Statistics, 2011, total excluding automotive fuel

[5]This number is now considered extremely suspect. Florêncio and Herley have shown that this type of estimate has been regularly over-estimated by using small sample sizes and failing to deal appropriately with outliers [16].

year from phishing. In a separate study, Florêncio and Herley studied when passwords were entered at unexpected websites and estimated that 0.4% of the Internet population is phished annually [15].

The other modus operandi of online banking frauds is to install keystroke-logging malware. In October 2010, the FBI arrested a crime ring alleged to be using the prolific Zeus malware, which harvests credentials from many banks. The FBI claims that the criminals attempted to steal $220 million, and successfully stole $70 million, though it is not clear what the time frame was for the thefts [14].

In addition to large botnet-based malware such as Zeus, some criminals have started using 'spear-phishing' to install targeted malware on machines used by small to medium sized businesses, typically targeting the CFO, the payroll department or the accounts payable department. According to the FBI, as of September 2011, they were investigating around 400 such cases of 'corporate account takeover' where criminals stole $85 million [51]. As these figures relate specifically to the USA rather than global losses (as was the case with Zeus) and as spear-phishing seems to be more developed against U.S. targets than in Europe, we'll estimate global losses at $300m.

Many defence costs also apply to other forms of online crime – antivirus, malware remediation programs, and so forth. There are some online-banking specific efforts, though, most notably the take-down industry whose firms contract with banks to remove phishing websites that impersonate the real thing. There are also vendors of chip authentication programme calculators, systems for generating one-time passwords via mobile phones, and so on, which might account for two dozen booths at a trade fair like RSA. Their collective turnover might be estimated at $500m globally. Adding in a similar amount for the banks' internal security development costs gives us an estimate of $1000m globally, or $50m for the UK, for securing online banking.

Regarding indirect costs, Eurostat's survey suggest that security concerns keep 16% of all individuals in the UK from carrying out online banking activities. An unofficial but plausible estimate puts the annual reduction of support cost at $70 per new online banking customer.[6] Combining both figures in a back-of-the-envelope calculation gives us a point estimate of £450 million in indirect cost for 2010, or $700m, shared between UK consumers and banks. This estimate is highly uncertain. It might be an upper bound because we cannot rule out that a fraction of the 16% stays away from online banking for more than one reason, and therefore might not adopt online banking even if security concerns were not an issue. Conversely, the cost savings seem to account for marginal costs only, i.e., assuming the bank maintains a network of branches anyway. If online banking became pervasive, the savings from closing branches could be much higher than the losses, especially if some of the losses can be socialised.

Indeed, an important research question here is whether countries with stronger consumer protection laws actually have more profitable banks, because of higher trust leading to more online banking leading to reduced costs of branches, staff and cheque handling, as well as increased transaction fees. From this year, the seventeen countries of the Eurozone are expected to publish uniform fraud statistics, and perhaps it will become feasible to get even bank CEOs to support stronger consumer protection. As UK consumer protection is lower than in the USA and the better Eurozone countries, we will scale up this notional economic loss from diminished confidence from $700m in the UK to $10bn globally rather than to $14bn.

[6] Source: `http://snarketing2dot0.com/2007/03/27/the-economics-of-online-banking/`, 2007.

3.3 In-person payment card fraud

The cost of physical payment card fraud can be estimated by subtracting Internet fraud from Financial Fraud Action UK's total fraud figure for 2010, that is, £230 million for UK-issued credit and debit cards. However some doubt remains about certain categories over whether they should be considered – at least partly – to be online crimes or not. Some frauds are clearly physical, for example the £67.4 million ($106m) due to face-to-face retail fraud; but this is still electronic (at least in the UK) as the great majority of card transactions are authorised online and use EMV. What's more, the common fraud mechanisms are technical in nature; villains use tampered PED terminals or ATM skimmers to capture card data and make forged cards that operate in fall-back mag-stripe mode. That accounts for the growth of 'counterfeit' fraud from 2005–2008; the deployment of EMV led to many more terminals accepting PINs which increased the opportunity for rogue devices to steal card and PIN data. The industry's response was that fewer and fewer UK ATMs accept mag-stripe fall-back transactions. This in turn led crooks to cash out overseas; the fall in 'counterfeit' UK transactions since 2008 has been matched by a growth in fraudulent overseas transactions, which amounted to £93.9 million ($147m) by 2010. In most cases, these frauds are facilitated by online communications between colluding fraudsters across the UK and abroad. So it seems sensible to account for 'online and electronic' fraud, a category that includes card fraud perpetrated in person.

The defence costs of EMV deployment are much harder to estimate. Retailers incurred significant expenditures in upgrading their terminal fleets; we have public figures from market leader Ingenico, which with 38% of the retail terminal market booked $907m of sales in 2010. This gives $2.4bn for the total market, and from experience we'd hazard a guess that the total cost of the systems are about three times that (when one adds the cost of integration, back-end systems and everything else). On the other hand, much of the cost of such systems can be ascribed to providing functionality rather than security. We'll estimate the defence cost of preventing card fraud as about equal to the cost of the terminals alone, namely $2.4bn.

3.4 Fake antivirus

Some cyber criminals altered the page contents of large numbers of web servers in such a way as to cause a visiting user to be presented with a pop-up window warning that their computer has been infected with malware, and that they should click OK to run antivirus software. When a user does click on the warning, fake antivirus software is installed that first disables any installed antivirus software and then issues repeated requests for payment. The only way to make these warnings go away is to pay up.

One group of researchers managed to get access to several internal databases run by three different criminal gangs perpetrating these crimes from 2008–2010 [54]. They found that the criminal groups had kept detailed records of conversion rates from installations to sales, along with the prices paid. The authors estimate that these three groups collectively earned $97 million per year. While there are probably more groups than the ones they studied, it is quite possible that these groups received the vast majority of the revenue attained from fake antivirus sales since the revenues from online crime are often concentrated among the most successful criminal groups.

3.5 Infringing pharmaceuticals

Advertising is one of the key avenues for monetizing online criminal platforms such as botnets. Criminals use a range of advertising vectors, including sending unsolicited bulk email (i.e., spam), manipulating search engine results (e.g., so-called 'black hat' search engine optimization), and abusing social communications platforms (e.g., Twitter spam, blog spam, etc.) to attract users to sites selling a range of goods and services. Typically, these criminal advertisers are loosely organized independent contractors who are paid on a commission basis for any customers they bring in, by sponsoring 'affiliate programs' [50].

Unlicensed pharmaceuticals are perhaps the goods most widely promoted using criminal advertising.[7] Pfizer sells a genuine Viagra pill for several dollars while factories in India will provide a generic version to merchants for under a dime; this large margin for arbitrage has made 'counterfeit' (more accurately, brand and/or patent-infringing) pharmaceuticals one of the best organized among underground businesses. Internet mail-order vendors support several thousand advertising affiliates and several dozen sponsoring affiliate programs.

Such activity incurs a range of indirect costs, many of them challenging to reason about in isolation. For example, pharmaceutical advertising dominates unsolicited bulk email and thus is a driver for the considerable expenses for anti-spam and content filtering products and services (a 2005 Frost and Sullivan report placed "World Content Filtering Revenues" at $1.31bn [19]). But these are not the only threats prevented by these technologies; even if counterfeit pharmaceuticals were removed from the market (say by better IP enforcement in China and India) it is not clear that the advertising channel would not be repurposed, and hence still drive the anti-spam industry. Similarly, estimates of lost time and productivity due to unwanted email or poor search quality, vary widely; they are both challenging to validate and to assign to a particular product category.

Looking at the direct risks to consumers, unregulated Internet pharmaceutical sales pose two potential liabilities: first, there is a risk of fraud — that a customer might order a drug and either not receive it or suffer subsequent charges to their credit card — and second there could be health risks due to poor quality and adulterated drugs. To the first point, there is very little empirical evidence to support the fraud hypothesis. Indeed, one of the authors' research groups has placed hundreds of pharmaceutical orders and has received products in all but a handful of cases and no unexplained fraud against the credit cards used [36, 30]. On the issue of health risks, while there are certainly concrete documented cases of individual harms [60], we are unaware of any systematic study of these risks or their overall costs to consumers. Moreover, recent studies of large-scale underground pharmaceutical programs documents that as much as a third of revenue is derived from *returning customers* — which seems unlikely if these customers were experiencing significant adverse reactions [42]. Of course, pervasive online availability of drugs such as opiates without prescription might exacerbate devastating addictions that impose substantial social costs.

Ironically, we possess better data about the criminal revenue brought in to the infringing vendors than about their direct or indirect costs to society. In one 2008 study, researchers manipulated the command and control channel of the Storm botnet to drive estimates of the underlying consumer conversion rate [29]. Extrapolating from this data, they suggested that this one botnet could drive revenues of $3.5 million per year for the pharmaceutical programs it advertised.

[7] In one recent report Symantec's MessageLabs division reported that pharmaceutical advertising represented roughly 80% of all spam email in June of 2010 [55] which is matched by similar data published by m86 security from the same time period [41]

A recent 2011 study provides a broader scope and a tighter bound on such sales using a technique to infer order volume based on the allocation of customer service identifiers over time [30]. Whilst placing a series of undercover purchases from each affiliate program, the researchers discovered that each customer was given a unique order number and that this number was incremented for each new order, across all orders from all advertisers for the affiliate program. They inferred a monthly order volume exceeding 82 000 across seven pharmaceutical affiliate programs. Using a mostly conservative approximation for order size, they further extrapolated that monthly revenue from these programs is roughly $6m.

However, a number of biases may affect this result. First, these seven programs clearly do not represent all organizations sponsoring infringing pharmaceutical sales online. For instance, researchers have found that other advertising vectors besides email spam, notably the manipulation of web search results, are also widely used to promote unauthorized pharmacies [35]. Nonetheless, the study estimating revenue does include the four largest affiliate programs, which represented over two-thirds of all email-advertised pharmaceutical URLs in a large-three month study of spam-based advertising [36]. Second, it does not account for differences in drug formulary. For example, sites selling restricted drugs such as steroids, opiates and stimulants can command a far larger revenue per order (one recent study demonstrated that carrying such drugs can double the revenue of a pharmaceutical program [42]). Finally, the methodology does not account for shopping cart abandonment just before the credit card is entered nor does it account for credit card declines (e.g., for fraud or insufficient funds).

Recently, a series of conflicts between major actors in the pharmaceutical affiliate program space has led to broad leakage of underlying financial records and transaction databases [32]. A recent 2012 study analyzing this data shows that, at its peak (2009), one of the largest pharmaceutical affiliate programs had annual gross revenues of $67M (of which 6.4% could be attributed to sales inside Great Britain) [42]. Moreover, by the contemporaneous order-number analysis mentioned earlier with this ground truth data for the same program, the authors were able to calibrate for biases due to declines and abandonment and establish an average revenue-per-order of $125. If we assume that these factors are consistent across the industry, then we estimate that the monthly revenue of counterfeit pharmaceutical sales from these top programs in 2010 was $8M per month. Moreover, based on activity in both email and web advertising channels we believe that these programs represent at very least a third of organized counterfeit pharmaceutical activity online at the time. Thus, we believe that annual 2010 revenues from sales of online pharmaceutical was likely bounded by $24M per month; $288M for the year.

These same two studies, include geo-located customer order data, placing the fraction of such orders originating in the UK at between 3% [30] and 6% [42]. Thus, despite the unique characteristics of the large US market, it seems robust to continue using our estimate that the UK share is 5%, reflecting the UK's share of world GDP.

Putting these measures together, we can estimate that UK consumers provided roughly $400,000 to the top counterfeit pharmaceutical programs in 2010 and perhaps as much as $1.2M per-month overall.[8].

To summarize, we'll estimate UK-originated criminal revenue at no more than $14m a year, and global revenue at $288m.

[8]Note, this this revenue is split among a number of actors. Roughly 35-40% is typically paid to advertisers (driving investments in botnets and other cybercrime support infrastructure), 20% goes to suppliers and shipping, and between 10-15% goes to bank discount and agent fees for payment card processing. After a range of indirect costs, net revenue for operators is typically 10-20% of gross[42]

3.6 Copyright-infringing software

The for-profit sale of counterfeit software, as with pharmaceuticals, is an advertising-based enterprise. The costs of distribution are negligible (particularly for online distribution) so the direct costs to criminals are primarily in sales acquisition (i.e., email spam, search engine optimisation, etc.) The societal costs are borne in the form of lost licensing revenues to copyright and brand holders (with the same confounding effects that we find in valuing losses due to counterfeit drug sales) while there are social benefits from people gaining value by using software that they would not have purchased at all at the full list price.

In 2004, the Business Software Alliance engaged Forrester Research to poll 1 000 Internet users in each of the U.S., U.K., France, Germany, Canada and Brazil concerning their attitudes towards email spam advertising [18]. Over 20% of UK respondents (versus 27% for the entire group) responded affirmatively that they had purchased software advertised in this manner. If we took all such advertisements to represent counterfeit software organizations and the survey to be both representative and accurate, then the online UK market for counterfeit software in 2004 would have been close to 12 million users.

A more recent 2011 study, using the empirical order number technique described earlier, estimated that three of the top five leading counterfeit software organizations together produced over 37 000 sales per month [30]. This metric is imperfect, since undoubtedly some of those orders did not complete and others were declined or refunded. Moreover, we do not know the monetary value of each such sale. However, if we assume the order rate estimate is correct and that the average software sale was $50, then this reflects an annual turnover of $22m worldwide for these organizations. Given that software prices have fallen in the past seven years (Microsoft's Office now costs tens of dollars rather than hundreds) and that ever more software is available free through cloud services, this fall should not be surprising.

3.7 Copyright-infringing music and video

Disputes over the value of copyright-infringing music and video have been many and vociferous, with the music industry blaming the Internet for declining CD sales. We have to treat such claims with caution. First, copyright infringement performed by individuals (as opposed to 'for profit') is a civil matter in the UK and most other countries, so does not fall under 'cybercrime'. Second, there has long been debate about whether illicit online copying actually depresses CD sales; an early study by Felix Oberholzer-Gee and Koleman Strumpf concluded that the people who did most file-sharing also bought the most CDs [48], while a thorough study by the Dutch government [24] concluded that copyright infringement through downloading pirated entertainment products gives a net social gain (for each dollar lost by the music industry, consumers gained two dollars' worth of value). On a broader scale, the transformation brought about by technology has meant that instead of people buying music an album at a time from a record company for £15 they now buy it a track at a time from Apple for 79p. Consumers get more music for their money and more musicians make a living. Job losses among music company middle managers are just the creative destruction inherent in technological progress.

As a result we do not think it is prudent to count the multibillion dollar claims of indirect losses made by music company advocates, but only the criminal gains made directly by gangs that operate downloading hubs. These are only in the hundreds of millions; for example, the recent raids on the Megaupload gang in Auckland who were claimed to be the world's largest led to asset seizures of the order of $50m [11]. That site had 150 million users and 50 million daily

visits; if we believe reports saying they had roughly a third of the market and that the $50m represented a year's profits, then we get a global figure for proceeds of crime of $150m.

3.8 'Stranded traveller' scams

Compromised webmail accounts are often used to send spam to the account owner's friends, a list of whom will be to hand in the address book. Spam blocking is often less stringently applied when there is regular communication, and the spam may leverage the social link, perhaps by providing a personal recommendation of a product. That aside, one of the most common uses of these compromised accounts is to operate the 'stranded traveller' scam.

In this scam, an email is sent along the lines of:

> "I write this with tears in my eyes. I had to travel to London at short notice and last night I was mugged at gun point. They have stolen all my cash, credit cards and mobile phone. Fortunately my passport and airline ticket was in my hotel room, but the manager will not let me check out until I settle my bill. Please will you spare me $1,900 to pay the hotel, I will reimburse you as soon as I get back."

If the recipient of the email is taken in, they will be instructed to send the money by Western Union. The sender may be reassured because they believe the money can only be picked up in London by the holder of an appropriate passport, but in practice the dollar amount will be below the limit for which government identity documents are needed, and the money can be picked up anywhere in the UK. A detailed account of the scam, from a victim's viewpoint, is given by Fallows [13].

The scammers exploit all the main webmail platforms, AOL, Gmail, Hotmail and Yahoo! along with Facebook. One of this paper's authors has unpublished 2010 data obtained by examining customer support reports to one of these companies. On average, the criminals were receiving one or two payments a day. Scaling up across the five platforms, and assuming (fairly arbitrarily) that only one in two losses was mentioned to the webmail company support team, means the annual turnover for this scam is approximately $10 million.

Assigned a loss to the UK is complex. Most of the victims were from the US and in 2010 most of the money was flowing towards the UK – although there are clear reasons to suppose its final destination was West Africa. So although this scam is relatively high profile, and makes for a good anecdote, the loss to the UK is most unlikely to exceed $1 million per annum.

3.9 'Fake escrow' scams

Another widely discussed but relatively uncommon scam is 'fake escrow'. Here the victim believes that they have won an online auction for a car or motorbike. The seller proposes that to safeguard both their interests they should use a third party escrow agent, which conveniently for the purchaser will also deliver the vehicle to their door. The seller will give the vehicle to the escrow/delivery company and pay the fees. The purchaser will pay money to the escrow company who will pay the seller and deliver the vehicle. However, despite having a convincing website with an online delivery tracking system, the escrow company is a sham and the putative purchaser will be perhaps $10 000 out of pocket.

There are around 100 active fake escrow websites at any given time [27], and the more competent fraudsters are believed to be 'selling' a car a week [52]. This puts the overall turnover in the

region of $200 million per annum. The scam operates to some extent in North America, but rather more in Europe. UK losses may be of the order of $10 million a year.

3.10 Advanced fee fraud

Advanced Fee Fraud (AFF) is sometimes called '419 fraud' after the relevant article of the Nigerian criminal code. It comes in a large number of formats, from the deceased dictator's family who want to smuggle millions of dollars, to scams where people win millions in lotteries they have never entered. The common feature of all of these frauds is that the victim must pay out a small amount of money (a tax, a bribe or just a bank account opening fee) in the expectation that this will release the large sum to them. If they pay out once then some other obstacle will arise and they will need to provide another advance fee – in extreme cases until they are personally bankrupt, or if they are repurposing their employer's funds, until their own fraud becomes apparent.

There are very strong links historically between AFF and West Africa, particularly Nigeria, going back to the days when it was conducted by letter and then fax. Email has made communications simpler, although the higher-value scams often involve face to face meetings, and occasionally even kidnapping – so at the top end, this is not purely a cybercrime.

As usual, figures are hard to come by, but in a 2006 Chatham House report [49], Peel set out a detailed account of Nigerian financial crime, which extends far beyond just 'cyber'. He quotes a 2004 CIFAS web page setting the cost to the UK economy at £150 million, but consulting the original (at archive.org) shows that the data on average loss (£31 000) came from a 2001 NCIS press release and – according to CIFAS – the same 2001 release gave the £150m figure as the losses for 2003 (which is presumably a typo for some earlier year).

Although it is possible to identify from press reports many individual cases of large losses, these are mainly in the US and they are scattered over many different years. There does not appear to be any reliable data at all on the overall loss to the UK in any particular year, with what figures there are being a summation of all cases worked by a particular police force, and perhaps then multiplied up to speculatively account for under-reporting.

In practice we suspect that the majority of losses in purely 'cyber' frauds are relatively small, having ourselves seen initial demands in lottery frauds of only £800. The prevalence and diversity of AFF emails in spam does however suggest that many criminals consider this a worthwhile line of activity. The higher profile of this fraud generally also makes it seem likely that it is more lucrative than the stranded traveller and fake escrow scams just discussed. So to avoid a gap in our tables we will pick a number of $50 million for UK losses, but we would be the first to admit that this figure is merely indicative and we have no real evidence to support it. We suspect it is rather on the high side.

3.11 PABX fraud

The Communications Fraud Control Association (CFCA) publishes data on fraud losses associated with telephony, both fixed and mobile. Their methodology is to survey experts from within the industry as to what proportion of turnover is lost to fraud, and – with some statistical adjustments to account for company size – thereby estimate the size of the problem. Their headline figure for 2011 is US$40bn [7]. Their methodology leads to some bizarre results – the overall loss is down by a third from their previous 2008 report, but 98% of the people they surveyed believed that fraud was static or increasing. However, their members do report real

losses, and just 34 panel members stated that that their companies had collectively lost US$2bn in the previous year.

The CFCA data distinguishes a range of crimes, from manipulation of the SS7 signalling system to hide the identity of a caller, through "clip on fraud" (physically connecting to someone else's phone line), to straightforward "subscription fraud" – failing to pay the bill. Of particular interest is "PABX fraud". The criminals reconfigure a company's telephone system (Private Automatic Branch Exchange) to accept incoming calls and relay them onward. They then sell phone cards (which can be little more than instructions on how to dial) to expat workers, who then 'call home' at the company's expense. This crime is decades old, and was once done by accessing a modem within the PABX that was used for remote maintenance, but PABXs are now placed on the Internet – and are often left with weak or default passwords.

The CFCA estimate for PABX fraud is US$4.96bn worldwide, US$1.28bn of which they believe occurs in Western Europe (so the UK share would be in the region of US$185m). The CFCA does not set out whether this is the wholesale or retail cost of the calls – defrauded companies can often renegotiate the actual payment they make to settle their unexpected bill.

3.12 Industrial cyber-espionage and extortion

Following the Detica report, UK government spokespersons have talked up the risk of espionage. One of them warned at a conference in Cambridge that the University had better invest more in cyber security or see its priceless intellectual property stolen. But Cambridge does not own priceless intellectual property; academics own the copyright in their own publications and software, and while the university does have the right of first refusal on patents that staff members choose to file, such patents cannot be 'stolen' once filed.

Similar comments can be made of other companies with valuable IP: drug firms' new products are may be vulnerable prior to filing, yet we're unaware of any case where a filing has been spoilt by unauthorised prior exposure. As for firms with valuable software, it is common for source code to be very widely available. Microsoft has tens of thousands of engineering staff with access while large numbers of outside organisations (from the Chinese government to some researchers at the University of Cambridge) have access to source code for Windows under a non-disclosure agreement. The Detica claim of £9.6bn of annual losses by 'companies that create significant quantities of IP or whose IP is relatively easy to exploit' has no obvious foundation.

The second part of Detica's claim is £7.6bn involving the theft and exploitation of non-IP related data such as companies involved in open tendering competititons or which can be affected by large share price movements. Again, there is no obvious foundation for this; however stock markets do have mechanisms to detect suspicious trades in advance of price-sentitive announcements, and if a leak from one company to another causes a tender for a public-sector IT project to be priced more keenly than would have otherwise been the case, then it's entirely unclear that the public is thereby harmed. Indeed there are frequent complaints about the oligopoly of large firms that win most public-sector business and there are officials at the Cabinet Office – the co-author of the Detica report – whose job it is to promote SME competition for public-sector supply and service contracts.

A third part is the claim that £2.2bn per annum is lost to extortion, with the comment that 'we believe this type of cybercrime goes largely unreported'. This is a very old and persistent claim made by security salesmen. One of us (Anderson) recalls working for a bank a quarter century ago and hearing it; even when it was truthfully denied, the salesmen persisted "we know it happens but you're not allowed to tell anyone" until escorted to the door for impertinence.

Extortion does occasionally happen – there was a widely reported case in 2004 when DDoS was used against online casinos and $4m was paid before the gang was arrested [39] – but like kidnapping, extortion is a hard crime to get away with, as money-laundering isn't trivial when the sender of the funds wishes to track down the recipient and has the active collaboration of the police.

In sum, because there is no reliable evidence of the extent or cost of industrial cyber-espionage and extortion, we do not include any figures for these crimes in our estimates.

3.13 Fiscal fraud

The Detica report also includes 'fiscal fraud committed against the Government' in its assessment of cybercrime. Certainly much tax and welfare fraud is committed by citizens who misrepresent their circumstances, and the UK (like other countries) is moving both tax filing and welfare claims online. Detica claims £2.2bn of fraud across tax, welfare, pensions, the NHS, other central government functions, and local government. They ascribed all such fraud to 'cyber' given that so many claims are now made online. That figure may well be justified but such fraud is nothing new.

In the USA, the IRS has made a determined effort to crack down on phishing gangs that impersonate it in order to trick people out of tax refunds, while in the UK, Her Majesty's Revenue and Customs (HMRC) appears to have made rather limited efforts. Following a news report that tax refund fraud was costing HMRC £600m a year [56], which was largely stolen online by foreign cyber criminals, we persuaded the MP for Cambridge, Dr Julian Huppert, to ask the following Parliamentary Question:

> Dr Huppert: To ask the Chancellor of the Exchequer what estimate he has made of the cost to the public purse of payments for tax refunds being fraudulently redirected as a result of websites that impersonate Government websites in the last three financial years.[86764]

The response, on behalf of the Chancellor of the Exchequer, was unhelpful:

> Mr Gauke: HM Revenue and Customs do not have an estimate of the cost of tax refund payments being fraudulently redirected as a result of websites that impersonate Government websites.

Rather than impersonate the tax office, criminals in the USA have been impersonating citizens by electronically filing fraudulent tax returns using stolen lists of names and Social Security numbers. The IRS claims the problem is widespread and growing. By their own estimation, in 2010 around 1.5 million tax returns were fraudulently filed, garnering refunds totalling $5.2bn [1]. By contrast, British tax authorities have taken steps to authenticate citizens who file returns electronically, physically mailing out passwords to the address on record that must be produced in order to file online.

In an off-the-record conversation with a senior civil servant, we learned that welfare cheating in Britain is 0.8% of the total expenditure, which is over £160bn. This figure is robust; they have done frequent drill-downs. It's overwhelmingly about misrepresentation of circumstances (undeclared partner / income / capital) and some of it is not even malicious (particularly elderly people who had put away a nest egg for a specific purpose and didn't think it part of their

capital). But most is fraud, and the rates vary widely from the state pension (under 0.1%) to means-tested benefits (over 4%). All of it will be 'computer crime' from 2013 when all claims will be done online; most of it already is. But it's almost unchanged from a few years ago when claims were in person. So welfare fraud adds £1.2bn to Britain's fraud figures.

Tax evasion is more slippery. Her Majesty's Revenue and Customs believe it's 2% but the figure is not robust and has been the subject of much internal debate in the civil service: different departments try to play it up, or down. As a result the numbers keep getting referred to the Office of National Statistics, who keep quibbling. This too is all rapidly 'becoming computer crime'. That will add a further £8bn. In passing, to put some of the numbers into context, we will note that so-called 'Missing Trader VAT fraud' or 'Carousel VAT fraud'[9] is estimated to have cost the UK £3 billion in 2005/6 [23]. At that time, this fraud had no substantial cyber component at all. Yet almost all VAT returns are online from this year (2012). Similarly, most income tax fraud is about misrepresentation of circumstances, income or capital, just like welfare fraud; the 'cyber' component about which Mr Gauke has no information might amount to a few hundred million. For consistency we'll put down the cost of tax fraud as £8bn or $12bn, which includes income tax, VAT and corporate taxes too – but we will put both welfare fraud and tax fraud separately at the bottom of the table to remind the reader that these are the figures for largely traditional frauds that now, because of electronic filing, fall within the EU definition.

3.14 Other commercial fraud

There are other types of commercial fraud from insider trading to embezzlement which will eventually, like fiscal fraud, be undeniably 'cyber'. Perhaps the largest category is control fraud, where the executives in charge of a company (or the ministers in charge of an economy) abuse their authority to loot it. There have been cases of control fraud with a 'cyber' element, such as the Equity Funding affair, but we have decided to exclude such frauds from this report for brevity as they are mostly concerned with the exercise of power in interpersonal and institutional relationships rather than by means of claims made relatively formally and mechanically through automated systems. What's more, in the case of control fraud (at least) the known countermeasures are not technical but concerned with institutional mechanism design – such as awarding company executives sufficient stock options to align their incentives with shareholders, and encouraging less developed countries to hold formal second-price auctions for access to their natural resources rather than permitting ministers to strike deals privately with foreign companies.

4 The Infrastructure Supporting Cybercrime

We now review the infrastructure supporting cybercrime. While these activities are often referred to directly as cybercrime, in fact they are used to enable lots of different crimes. Consequently, we estimate the infrastructure's costs separately so as to avoid double counting.

[9] In a VAT fraud goods such as mobile phones are imported into the UK. They are sold on within the UK, VAT paid on this sale (15% to 20% at various times) which should be paid to the taxman is pocketed by criminals who shut down the company and disappear. The recipient can now re-export the phones and claim back the VAT (doubling the criminal's take) – and the same batch of goods can then be cycled round again and again, hence the carousel term.

4.1 Botnets

Botnets are a key part of the infrastructure for cybercrime. A botnet is a network of thousands, sometimes even millions, of machines that have been infected with malware, putting them under the remote control of criminals. The 'botnet herders' who assemble these collections of machines may either use them for crime directly or rent them out to others to operate. The operator will typically send instructions to his infected machines to download further malware to implement specific attacks. Botnets provide a versatile platform for a variety of criminal business models, including sending spam, committing click fraud, harvesting account credentials, launching denial-of-service attacks, installing scareware and phishing.

It is the criminal business models that generate the revenue, but because the botnets provide a platform for them, they have value within the criminal economy, as we can see in underground markets where botnets are sold and rented. The cost of the criminal business models that use botnets are discussed elsewhere in this paper; as for the botmasters' turnover, Herley and Florêncio estimated in 2009 an upper bound to botnet herders' income of 50c per machine per annum, so that a 20 000-machine botnet earned its herder some $190 a week [21]. That was an upper bound, and botnets seem to have become bigger since then; if we assume 50 million bots worldwide, we'll estimate annual herder income in the single millions per year, and that is too low a figure for us to include it in our summary table.

There are also the costs the botnets themselves inflict on society. These losses occur first and foremost in the cost of dealing with the infected machines. The costs are distributed across different actors, most notably the owners of those machines, ISPs (in the sense of access providers) and hosting providers. Recent empirical analysis showed that around 80% of all infected machines are located in the networks of ISPs [59]. Of the remaining 20%, the largest share could be attributed to hosting providers – i.e., infected servers. This picture is evolving, however, and may increasingly include mobile devices.

4.2 Botnet mitigation by consumers

There are only snippets of evidence about the costs associated with botnet mitigation. Currently, there is no single authoritative data source to identify the total population of infected machines around the world, and each source has its own strengths and weaknesses.[10] Two robust and independent estimates both suggest that a little over one million British households have had a machine in a botnet at least once per year. The first estimate comes from Microsoft, which they say is based on telemetry from over 600 million machines worldwide. In the first half of 2010, their Malicious Software Removal Tool cleaned up around 500 000 bots in the UK [44]. They did not produce a similar number for the second half, but overall malware infections in the U.K. did rise slightly compared to the first half, so it is likely that the total for the year lies just over one million [43]. Following a completely different measurement approach, a study of the Dutch market, done in close collaboration with the ISPs, compared Dutch infection levels to those in the UK and other countries [57]. In those metrics, the UK is in the same ball park as the Netherlands: in 2010, around 6% of the 19 million UK broadband subscribers had a machine in a botnet at some point during the year. That translates to 1.1 million subscribers.

[10] Many estimates of the total number of machines that are affected have relied on counting the number of unique IP addresses that show up in botnet activity. We now know that this overestimates the size of the problem, often by an order of magnitude. Dynamic IP address allocation can cause the same infected machine to show up under many different IP addresses. When the Dutch police took down Bredolab, it was claimed that the botnet had infected 30 million machines in about two years. In reality, the evidence suggests that it was around 3 million machines.

It is much less clear, however, what cleaning up these one million infected machines costs. Many infections are cleaned up by the generic countermeasures of automatic security updates and anti-virus software, without much user involvement. Those would fall under indirect costs. We do not really know how often users clean up machines themselves and at what cost. In a 2007 survey by Consumers Union, a U.S. consumer protection organization, residential users reported to their total repair cost from malware were around US $5 billion in the past year – or around $100 per household/broadband subscriber [8]. In addition to clean-up, this includes the cost of replacing a poorly functioning, malware-ridden computer with a new one, even though it seems incorrect to fully attribute the price of a new machine to the problem of malware. Furthermore, the reliability of these surveys is highly questionable, a problem which is exacerbated by the fact that underlying data and methodology are not made public. Furthermore, the cost of PCs has fallen sharply in the last five years, from almost a thousand pounds to a few hundred. We will therefore be ultra-cautious and estimate a rough current equivalent for the UK as $500m. To put this in perspective, it sets the average clean-up cost per household per year at less than the cost of one hour of end-user time valued against the UK GDP per capita.

4.3 Botnet mitigation by industry

Another loss is borne by ISPs and hosting providers, who may have to act against infected machines in their networks.[11] The scale at which such mitigation efforts take place is highly variable. Finnish ISPs, for example, act on most infected machines that are detected, whereas in in UK, As in most other Western countries, ISPs only tackle a small fraction of the infected population. We have no data on how much these efforts cost. To some extent they can be automated, but the largest cost is customer support. A recent German initiative set up a national call centre to deal with botnet mitigation. In the first year of its operation, it notified 315 518 end users that they owned an infected machine [20] – a fraction of the infected population. Most notified users ran an automatic clean-up tool; less than 1% of them needed customer support over the phone, with the average call lasting for about 15 minutes. Operating the centre cost about 2 million euro in funding for its setup and first year of operations. Note that this cost does not cover the whole problem, as comparative infection measurements suggest the centre notified around a quarter of the infected population. If all infected customers were to be notified, the cost would rise, but still remain well under 10 million, as we expect that the marginal costs of notifying and helping additional users to diminish. While there are no comparable figures for the UK, it seems reasonable to assume that the cost there are similar or lower, in other words: in the single millions per year. A more fully developed mitigation strategy, like the one in Finland, is probably in the same ballpark. It may cost more at first, but automation can take over part of the process and, once the infection rate diminishes, so do the support costs of customers.

A further cost is that of botnet mitigation by commercial firms other than service providers (and banks and retailers, whose $7bn anti-fraud measures we account for above). Figures for the total information security industry are difficult, with some reports suggesting of the order of $20bn [6] or even more. Symantec alone has turnover of $6bn, but that's everything, not just their antivirus business; we'll estimate antivirus expenditure worldwide at $3.4bn. It's a bit harder to reckon how much of industry's infosec costs to ascribe to generic defences (over and above the specific payment-system defences deployed by banks and merchants); sysadmins mostly do other things than security, and internal controls have other purposes than limiting the damage an infected machine can do. In order to be ultra-cautious, we'll ascribe a global figure

[11] Some of these costs are directly related, and proportional, to the infection of machines. ISPs also bear indirect losses and more general defence costs, which do not vary with the outbreak of botnet infections.

of $10bn to generic cybercrime defences by companies worldwide. This sets the corporate costs of mitigating botnets to be equal to the costs borne by individuals. We don't know whether this is right; corporates are more concerned about security, but also more efficient at providing it. So we'll hazard a figure of $10bn, bearing in mind that only the order of magnitude is probably right.

4.4 Other botnet mitigation costs

The indirect losses due to botnets are much more dispersed; many losses mentioned elsewhere in the paper are relevant here as well. A more specific effect is that malware may motivate end users, platform owners and service providers to move away from general purpose computers towards more controlled platforms, such as Apple's model of iOS and the App Store. This may help innovation in the short run, but in the end it might reduce innovative capacity via locked-down devices, new concentrations of market power and less user autonomy [62]. The economic effects of this are unpredictable, though; if Apple wins at the expense of Microsoft, it's best to see this as the normal operation of capitalism rather than trying to interpret it as a security issue. After all, Android in turn is eating some of Apple's market. That said, if the security issues support an overall trend towards more restrictions on end users devices, this may reduce the potential for innovation and generate substantial societal opportunity costs.

Defence costs are more straightforward; many actors in the ecosystem bear them. End users, ISPs and software vendors all invest in technical measures to protect against infection. While numerous problems remain, end-user adoption of antivirus software is actually very high. The cost of this software may be borne by end users, by access providers (who bundle it with the subscription) or by platform vendors like Microsoft, who incorporate it in the platform. There are also vendors of antivirus solutions that provide them for free to home users, and cross-subsidise this from corporate licenses. The total cost of antivirus defence mechanisms is unknown, but we could assume from the Eurostat 2010 ICT survey that 88% of all households with a broadband subscription use at least one of these products. A conservative estimate would put the worth of a single license at $10, ignoring for a moment which actor actually bears this cost. For the UK, these assumptions estimate the total cost of antivirus countermeasures at around $170 million.

Other general defence costs are more difficult to estimate. Software vendors constantly patch their products against vulnerabilities that can be exploited by malware. Anecdotal evidence suggests that for mission-critical software, such as enterprise databases, the cost of a single patch development cycle can run up to a million dollars [58]. Similarly, the deployment of the patch within companies is also costly. By way of illustration: every time Google patches the kernel on the workstations of its employees, the subsequent reboot of the machines costs them over $1 million in lost productivity [4]. Further deployment costs include testing and assuring the patches before rolling them out. All of this suggests that for the whole software market, the cost of patching will be in the hundreds of millions, probably more. However, the part of this cost that can be attributed to the UK will probably be at most its share in global GDP, as its software industry is proportionally smaller than that in the USA. If we assume, for illustrative purposes, that the global cost of patching is $1 billion per year, this would mean the UK bears $50 million of this. This does not include the costs of deployment, which are borne by the end users.

Finally, we should also mention the cost of law enforcement as a general defence cost. Investigations aimed at taking down botnets and prosecuting the criminals behind them are very time-consuming and require costly specialists. That being said, few cases are investigated in depth. In the last two years, there have been only a handful of botnet takedowns: Kelihos, DNS

Changer, Rustock, Pushdo/Cutwail, Bredolab, Coreflood and Waledec. None of these seem to have had a substantial involvement from UK law enforcement agencies. We understand that the UK police have received an extra £30 million for the next four years which will let them open three regional centres to support cybercrime and forensic investigations: say another $10m raising UK police cyberbudgets to $15m a year. Meanwhile the US spends about $100m at the Federal level (FBI, Secret Service, FTC and NCFTA) and we may assume the same again at state level. The US is by far the major player in cyber enforcement, and seems to do about half the work; so we'll estimate global law-enforcement expenditures at $400m.

4.5 Pay-per-install

Wondracek and colleagues studied links between the pay-per-install business and the porn industry [61]. A pay-per-install operator is a criminal who infects PCs to order; for example, they charge $130 to install malware on 1000 PCs in the USA (the prices for Asia are much lower – as low as $3 for China). This study unearthed a whole ecosystem of shady services, with business links between adult pay sites, free sites, link collections, traffic brokers, search engines and redirector services. As another example, $160 bought 49 000 visitors, of whom more than 20 000 were vulnerable to at least one known vulnerability. They concluded that although not all porn sites are crooked, many are; the underground economy is a major financier of the adult business. A further study by Caballero, Grier, Kreibich and Paxson found that 12 of the world's top 20 malware families used PPI services for distribution [5].

If 50m machines are in botnets, with an average infection duration of 6 months, then 100m machines are infected every year. If half of these are done by PPI firms at an average cost of $50 per thousand, that's a turnover of $2.5m which lies below our reporting threshold. In fact, Caballero and colleagues caution that there's little point in cleaning up a botnet if the herder can rebuild his asset by very modest payments to PPI services.

5 Fitting the Estimates into the Framework

Previous studies of cybercrime have tended to study quite different things and were often written by organisations (such as vendors, police agencies or music industry lawyers) with an obvious 'agenda'. The subject is difficult because definitions are hard; much fraud that used to be conducted on paper or face-to-face (such as tax and welfare fraud) is now 'online' and these traditional frauds are much larger in volume and value terms than the new purely 'computer' frauds. Also, there is a significant amount of fraud 'in between' the traditional and the new, such as payment card fraud. This type of fraud began to change twenty years ago, but the move online and the transition from magnetic-stripe to EMV technology have quite changed the modus operandi. We've called this 'transitional' fraud for want of a better name.

In this report we have gone through the main types of fraud, whether traditional, transitional or modern. For each modus operandi we've collected the best figures from current research, and where none were available we've done what we could to provide neutral estimates. We collate our estimates here in Table 1. The numbers in bold are the ones we observed or estimated directly, whether UK figures or global ones; where we have only one of the two, the other is scaled on the basis that the UK is 5% of the world by share of GDP. In some cases, the scale is different for specific reasons that are mentioned in the text.

While we are relatively happy to scale down global fraud figures to obtain UK-specific estimates, we urge caution in interpreting the global estimates where we could only extrapolate from UK

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

Type of cybercrime	UK estimate	Global estimate	Reference period	Criminal revenue	Direct losses	Indirect losses	Defence cost
Cost of genuine cybercrime							
Online banking fraud							
– phishing	$16m	**$320m**	2007	$\times^{?}$	$\times^{?}$		
– malware (consumer)	$4m	**$70m**	2010	$\times^{\downarrow}$	$\times^{\downarrow}$		
– malware (businesses)	$6m	**$300m**		$\times^{\downarrow}$	$\times^{\downarrow}$		
– bank tech. countermeasures	$50m	**$1 000m**	2010				$\times^{?}$
Fake antivirus	$5m	**$97m**	2008–10	$\times$	$\times$		
Copyright-infringing software	**$1m**	**$22m**	2010	$\times$	$\times$		
Copyright-infringing music etc	$7m	**$150m**	2011	$\times^{\downarrow}$			
Patent-infringing pharma	**$14m**	**$288m**	2010	$\times$			
Stranded traveller scam	$1m	**$10m**	2011	$\times^{\downarrow}$			
Fake escrow scam	$10m	**$200m**	2011	$\times^{\downarrow}$			
Advance-fee fraud	**$50m**	$1 000m	2011	$\times^{\downarrow}$			
...							
Cost of transitional cybercrime							
Online payment card fraud	**$210m**	$4 200m	2010		(×)		
Offline payment card fraud							
– domestic	**$106m**	$2 100m	2010		$\times^{\downarrow}$		
– international	**$147m**	$2 940m	2010		$\times^{\downarrow}$		
– bank/merchant defence costs	$120m	**$2 400m**	2010				$\times^{\downarrow}$
Indirect costs of payment fraud							
– loss of confidence (consumers)	**$700m**	$10 000m	2010			$\times^{?}$	
– loss of confidence (merchants)	**$1 600m**	$20 000m	2009			$\times^{?}$	
PABX fraud	**$185m**	**$4 960m**	2011	×	$\times^{\downarrow}$		
...							
Cost of cybercriminal infrastructure							
Expenditure on antivirus	**$170m**	$3 400m	2012				×
Cost to industry of patching	$50m	**$1 000m**	2010				$\times^{?}$
ISP clean-up expenditures	**$2m**	$40m	2010			$\times^{?}$	
Cost to users of clean-up	**$500m**	$10 000m	2012			$\times^{?}$	
Defence costs of firms generally	$500m	**$10 000m**	2010				$\times^{?}$
Expenditure on law enforcement	**$15m**	$400m	2010				×
...							
Cost of traditional crimes becoming 'cyber'							
Welfare fraud	**$1 900m**	$20 000m	2011	×	(×)		
Tax fraud	**$12 000m**	$125 000m	2011	$\times^{?}$	(×)		
Tax filing fraud	-	**$5 200m**	2010	×	(×)		
...							

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

figures. Extrapolating from a sample representing 5% of world GDP can exaggerate the impact of local variation in fraud. The media claim, for example, that tax fraud is higher in Greece, and medical benefits fraud higher in the USA; we do not try to investigate such variance here. Ideally, global surveys could be undertaken for the categories where we lack global estimates. Nonetheless, we include the extrapolated figures in the table when necessary to aid policymakers while such data is not available.

Readers may be wondering why the table does not include any totals. It is after all a simple matter to add up the "Cost of genuine cybercrime" section to give a US$170m figure. But since this 'exact' value is less than the reported cost of card fraud in the very next row of the table, and that in turn is dwarfed by many other figures in later rows – and many of these are extremely rough estimates – we believe it is entirely misleading to provide totals lest they be quoted out of context, without all the caveats and cautions that we have provided.

Our work has its limitations. Inter alia, it gives a static view of the economics of cybercrime while the dynamics also matter. The development of the dark market in carding data, crimeware, botnet rental and other illegal services has, as we have just noted, made only a small contribution to the total figure we have presented. Nevertheless, it has enabled significant growth in other crime categories in the period since such markets got organised in the mid-2000s. However we believe that our work is a principled start to being able to measure the cost of cybercrime. We propose to continue updating our estimates, and to produce new versions of this paper every few years.

6 Conclusion

The data we have collected indicates that, in terms of the measurable costs:

- Traditional frauds such as tax and welfare fraud cost each of us as citizens a few hundred pounds/euros/dollars a year.[12] With such crimes, the costs of defences, and of subsequent enforcement, are much less than the amounts stolen.
- Transitional frauds such as payment card fraud cost each of us as citizens a few tens of pounds/euros/dollars a year. Online payment card fraud, for example, typically runs at 30 basis points, or 0.3% of the turnover of e-commerce firms. Defence costs are broadly comparable with actual losses, but the indirect costs of business foregone because of the fear of fraud, both by consumers and by merchants, are several times higher.
- The new cyber-frauds such as fake antivirus net their perpetrators relatively small sums, with common scams pulling in tens of cents/pence per year per head of population. In total, cyber-crooks' earnings might amount to a couple of dollars per citizen per year. But the indirect costs and defence costs are very substantial – at least ten times that. The clean-up costs faced by users (whether personal or corporate) are the largest single component; owners of infected PCs may have to spend hundreds of dollars, while the average cost to each of us as citizens runs in the low tens of dollars per year. The costs of antivirus (to both individuals and businesses) and the cost of patching (mostly to businesses) are also significant at a few dollars a year each.

[12]The precise choice of currency isn't important given the accuracy of the figures available to us; we can be reasonably sure we've got the orders of magnitude right, and often the binary order of magnitude, but not much beyond that

This brings us to an interesting question. Traditional acquisitive crimes, such as burglary and car theft, tend to have two properties. The first is that the impact on the victim is greater in financial terms than either the costs borne in anticipation of crime, or the response costs afterwards such as the police and the prisons. For example, Canada estimated victim costs of $47bn, criminal justice system costs of $13bn and defence costs of $10bn across its economy as a whole in 2003 [26]. Other countries use different measures but the broad picture is similar.

Drilling down further into the victim costs, we find that for nonviolent crimes the value of the property stolen or damaged is much greater than the cost of lost output, victim services or emotional impact. With the new cybercrimes, the pattern is much more like robbery, where (according to UK Home Office 2005 figures) only £109 is stolen but the additional costs include £483 for health services, £1 011 for lost output, and a whopping £3 048 for distress [22].

It may be worth noting that the criminal justice system recognises the quite disproportionate social costs of robbery as opposed to burglary; the typical robbery incurs £2 601 of criminal justice system costs compared with a typical burglary, where a much larger amount (£846) is stolen and yet less than half as much (£1 137) is spent on justice. Yet while robbers get longer sentences than burglars do, cyber-crooks get shorter ones. This is probably because cyber-crimes, being impersonal, evoke less resentment and vindictiveness. Indeed, the crooks are simply being rational: while terrorists try to be annoying as possible, fraudsters are quite the opposite and try to minimise the probability that they will be the targets of effective enforcement action.

Why does cyber-crime carry such high indirect and defence costs? Many of the reasons have been explored in the security-economics literature: there are externalities, asymmetric information, and agency effects galore. Globalisation undermines the incentives facing local police forces, while banks, merchants and service providers engage in liability shell games. We are also starting to understand the behavioural aspects: terrorist crimes are hyper-salient because the perpetrators go out of their way to be as annoying as possible, while most online crooks go out of their way to be invisible. The possible policy remedies have also been discussed at length, from better statistics to better international cooperation [2, 46]. But what's the priority?

The straightforward conclusion to draw on the basis of the comparative figures collected in this study is that we should perhaps spend less in anticipation of computer crime (on antivirus, firewalls etc.) but we should certainly spend an awful lot more on catching and punishing the perpetrators.

A final point is that, according to the British Crime Survey, some 2% of respondents reported suffering a traditional acquisitive crime such as burglary or car theft, while more than double that number suffered fraud. The survey did not disambiguate the online and electronic frauds of interest here from the door-to-door and boiler-house variety, but the former probably accounted for most of it. A special module on IT security of the 2010 Eurostat ICT survey completes this picture. Ranking all 27 EU countries by online user's concerns, the UK ranks sixth for virus infections, fourth for spam, and second behind Latvia for the three remaining threats: personal data abuse and privacy violation; financial losses caused by phishing and pharming; and financial losses due to fraudulent payment card use. When looking at the self-reported actual experience of threats, the picture becomes more differentiated. On the one hand, UK residents exactly match the EU average for virus infections and privacy threats, and they seem to receive less spam than the average European. On the other hand, the UK ranks second for financial losses caused by phishing and pharming attacks, and first for payment card fraud, which affected 5% of the UK's online population.

If this interpretation is correct, then cybercrime is now the typical volume property crime in the UK, and the case for more vigorous policing is stronger than ever.

References

The URLs in this bibliography were all valid when last accessed on February 24, 2012.

[1] Lizette Alvarez. With personal data in hand, thieves file early and often. *New York Times*, May 2012. http://www.nytimes.com/2012/05/27/us/id-thieves-loot-tax-checks-filing-early-and-often.html.

[2] Ross Anderson, Rainer Böhme, Richard Clayton, and Tyler Moore. *Security Economics and the Internal Market*. January 2008. http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec.

[3] Erik Brynjolfsson and Adam Saunders. *Wired For Innovation: How Information Technology Is Reshaping the Economy*. The MIT Press, October 2009.

[4] Thomas Bushnell. How google developers use ubuntu. http://www.ubuntuvibes.com/2012/05/how-google-developers-use-ubuntu.html, 2012.

[5] Juan Caballero, Chris Grier, Christian Kreibich, and Vern Paxson. Measuring Pay-per-Install: The Commoditisation of Malware Distribution. In *Proceedings of the 20th USENIX conference on Security*, SEC'11, Berkeley, CA, USA, 2011. USENIX Association.

[6] Canalys Inc. Enterprise security market to exceed $22 billion in 2012, December 2011. http://www.canalys.com/static/press_release/2011/canalys-press-release-201211-enterprise-security-market-exceed-22-billion-2012.pdf.

[7] Communications Fraud Control Association. 2011 global fraud loss survey. http://www.cfca.org/fraudlosssurvey/, 2011.

[8] Consumers Union. State of the 'net' survey '07. *Consumer Reports*, 9:28–34, 2007.

[9] Lorrie Faith Cranor, editor. *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit 2007, Pittsburgh, Pennsylvania, USA, October 4–5, 2007*, volume 269 of *ACM International Conference Proceeding Series*. ACM, 2007.

[10] Detica and Office of Cyber Security and Information Assurance. The cost of cyber crime, February 2011. http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime.

[11] Clive Eliot. Kim Dotcom – Pirate or Enabler? http://www.nzherald.co.nz/auckland-region/news/article.cfm?l_id=117&objectid=10784190, 2012.

[12] European Commission. Towards a general policy on the fight against cyber crime, May 2007. COM(2007) 267 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF.

[13] James Fallows. Hacked! *The Atlantic*, November 2011. http://www.theatlantic.com/magazine/archive/2011/11/hacked/8673/.

[14] Federal Bureau of Investigation. International cooperation disrupts multi-country cyber theft ring. *Press Release*, October 2010. http://www.fbi.gov/news/pressrel/press-releases/international-cooperation-disrupts-multi-country-cyber-theft-ring.

[15] Dinei Florêncio and Cormac Herley. Evaluating a Trial Deployment of Password Re-Use for Phishing Prevention. In Cranor [9], pages 26–36.

[16] Dinei Florêncio and Cormac Herley. Sex, Lies and Cyber-crime Surveys. In *Proceedings (online) of the Workshop on Economics of Information Security*, June 2011. http://research.microsoft.com/pubs/149886/SexLiesandCybercrimeSurveys.pdf.

[17] Linda Foley, Karen Barney, Jay Foley, James Leeii, Julie Fergerson, Matthew Sarrel, Charles Nelson, and Mari Frank. Identity Theft: The Aftermath 2009, 2010. http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2009_20100520.pdf.

[18] Forrester Data. Consumer Attitudes Toward Spam in Six Countries. http://www.bsacybersafety.com/files/Forrester_Consumer_Spam.pdf, December 2004.

[19] Frost and Sullivan. Increasing Security Needs of Enterprises to Fuel Growth in the World Content Filtering Market. *Press Release*, October 2006. http://www.frost.com/prod/servlet/press-release.pag?Src=RSS&docid=84071018.

[20] Mümin Gözenoglu and Randolph Morawe. The German Anti-Botnet Advisory Center. Presentation at 'Internet Security Days', 13–15 September 2011, Brühl, Germany, http://www.internet-security-days.com/templates/downloads/session-2011/110913_Goezenoglu_Morawe_ABBZ.pdf, 2011.

[21] Cormac Herley and Dinei Florêncio. Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy. In *Proceedings (online) of the Workshop on Economics of Information Security*, June 2009. http://research.microsoft.com/pubs/80034/nobodysellsgoldforthepriceofsilver.pdf.

[22] Home Office. The economic and social costs of crime against individuals and households 2003–4. http://webarchive.nationalarchives.gov.uk/20110218135832/http://rds.homeoffice.gov.uk/rds/ecom_soc_cost.html, 2005.

[23] House of Lords European Union Committee. Stopping the carousel: Missing trader fraud in the EU. 20th Report of Session 2006-07, May 2007.

[24] Annelies Huygen, Paul Rutten, Sanne Huveneers, Sander Limonard, Joost Poort, Jorna Leenheer, Kieja Janssen, Nico van Eijk, and Natali Helberger. Ups and downs – Economic and cultural effects of file sharing on music, film and games. TNO report 34782, http://www.ivir.nl/publicaties/vaneijk/Ups_And_Downs_authorised_translation.pdf, February 2009.

[25] Martin Innes. Signal crimes and signal disorders: notes on deviance as communicative action. *British Journal of Sociology*, 55:335–355, September 2004.

[26] Institute for the Prevention of Crime. Cost of the criminal justice system. http://www.socialsciences.uottawa.ca/ipc/eng/cost_of_the_criminal_justice_system.asp, 2012.

[27] Henry Irish. Machine learning to classify fraudulent websites. 3rd Year Project Report, Computer Laboratory, University of Cambridge, 2012.

[28] Carl Kalapesi, Sarah Willersdorf, and Paul Zwillenberg. The Connected Kingdom: How the Internet is Transforming the U.K. Economy. http://www.connectedkingdom.co.uk/the-report, October 2010.

[29] Chris Kanich, Christian Kreibich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson, and Stefan Savage. Spamalytics: An empirical analysis of spam marketing

conversion. In *Proceedings of the ACM Conference on Computer and Communications Security*, October 2008.

[30] Chris Kanich, Nicholas Weaver, Damon McCoy, Tristan Halvorson, Christian Kreibich, Kirill Levchenko, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage. Show Me the Money: Characterizing Spam-advertised Revenue. In *Proceedings of the USENIX Security Symposium*, San Francisco, CA, August 2011.

[31] Akif Khan and James Hunt. UK Online Fraud Report 2012. `http://forms.cybersource.com/forms/FraudReport2012UKUKwebwww2012`, 2012.

[32] Brian Krebs. SpamIt, Glavmed Pharmacy Networks Exposed. Krebs on Security Blog, `http://krebsonsecurity.com/2011/02/spamit-glavmed-pharmacy-networks-exposed/`, February 2011.

[33] Brian Krebs. Who's behind the worlds largest spam botnet? Krebs on Security Blog, `http://krebsonsecurity.com/2012/02/whos-behind-the-worlds-largest-spam-botnet/`, February 2012.

[34] Dmitri Kuksov. Buyer Search Costs and Endogenous Product Design. *Marketing Science*, 23(4):490–499, 2004.

[35] N. Leontiadis, T. Moore, and N. Christin. Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade. In *Proceedings of USENIX Security 2011*, San Francisco, CA, August 2011.

[36] Kirill Levchenko, Neha Chachra, Brandon Enright, Mark Felegyhazi, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Andreas Pitsillidis, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage. Click Trajectories: End-to-End Analysis of the Spam Value Chain. In *Proceedings of the IEEE Symposium on Security and Privacy*, May 2011.

[37] Michael Levi. Social reactions to white-collar crimes and their relationship to economic crises. In Mathieu Deflem, editor, *Economic Crisis and Crime*, pages 87–105. The JAI Press/Emerald, 2011.

[38] Michael Levi and John Burrows. Measuring the impact of fraud in the UK: A conceptual and empirical journey. *British Journal of Criminology*, 48:293–318, 2008.

[39] John Leyden. Russian bookmaker hackers jailed for eight years. `http://www.theregister.co.uk/2006/10/04/russian_bookmaker_hackers_jailed/`, 2006.

[40] Ethan Lieber and Chad Syverson. Online vs. Offline Competition. In Martin Peitz and Joel Waldfogel, editors, *The Oxford Handbook of the Digital Economy*. 2012.

[41] M86 Security Labs. Canadian Pharmacy no Longer King. `http://www.m86security.com/labs/traceitem.asp?article=1316`, May 2010.

[42] Damon McCoy, Andreas Pitsillidis, Grant Jordan, Nicholas Waver, Christian Kreibich, Brian Krebs, Geoffrey M. Voelker, Stefan avage, and Kirill Levchenko. PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs. In *Proceedings of the USENIX Security Symposium*, Bellevue, WA, August 2012.

[43] Microsoft Inc. Microsoft security intelligence report, volume 10, 2010. `http://www.microsoft.com/security/sir/`.

[44] Microsoft Inc. Microsoft security intelligence report, volume 9, 2010. http://www.microsoft.com/security/sir/.

[45] Tyler Moore and Richard Clayton. Examining the impact of website take-down on phishing. In Cranor [9], pages 1–13.

[46] Tyler Moore, Richard Clayton, and Ross Anderson. The economics of online crime. *Journal of Economic Perspectives*, 23(3):3–20, Summer 2009.

[47] National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. W.W. Norton, New York, 2004.

[48] Felix Oberholzer-Gee and Koleman Strumpf. File-sharing and copyright. Harvard Business School Working Paper 09-132 http://www.hbs.edu/research/pdf/09-132.pdf, 2009.

[49] Michael Peel. Nigeria-Related Financial Crime and its links with Britain. Chatham House Report, November 2006.

[50] Dmitry Samosseiko. The Partnerka – What is it, and why should you care? In *Proc. of Virus Bulletin Conference*, 2009.

[51] Gordon Snow. Cyber security: Threats to the financial sector. *Testimony before the House Financial Services Committee*, September 2011. http://financialservices.house.gov/UploadedFiles/091411snow.pdf.

[52] 'Sodano'. Personal communication, 2007.

[53] Joseph E. Stiglitz and Linda J. Bilmes. *The Three Trillion Dollar War: The True Cost of the Iraq Conflict*. W.W. Norton, New York, 2008.

[54] Brett Stone-Gross, Ryan Abman, Richard A. Kemmerer, Christopher Kruegel, Douglas G. Steigerwald, and Giovanni Vigna. The underground economy of fake antivirus software. In *10th Workshop on the Economics of Information Security*, Fairfax, VA, June 2011.

[55] Symantec. MessageLabs Intelligence Report, June 2010.

[56] Jerome Taylor. Overseas cyber-crimewave taking £600m a year from the taxman. *The Independent*, December 2011.

[57] Michel Van Eeten, Hadi Asghari, Johannes M. Bauer, and Shirin Tabatabaie. *Internet Service Providers and Botnet Mitigation: A Fact-Finding Study on the Dutch Market*. The Hague: Ministry of Economic Affairs, 2011. http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/01/13/internet-service-providers-and-botnet-mitigation.html.

[58] Michel Van Eeten and Johannes M. Bauer. Economics of malware: Security decisions, incentives and externalities. Technical Report OECD STI Working Paper 2008/1, OECD, Paris, 2008. http://www.oecd.org/dataoecd/53/17/40722462.pdf.

[59] Michel Van Eeten, Johannes M. Bauer, Hadi Asghari, and Shirin Tabatabaie. The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data. Technical Report s0 STI Working Paper 2010/5, OECD, Paris, 2010. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/DOC(2010)5&docLanguage=En.

[60] Vancouver Sun. Online drugs can prove deadly: coroner. http://www.canada.com/vancouversun/news/story.html?id=ddadbf8a-bdac-45c4-a566-36acd8ffd72b, March 2007.

[61] Gilbert Wondracek, Thorsten Holz, Christian Platzer, Engin Kirda, and Christopher Kruegel. Is the Internet for Porn? An Insight Into the Online Adult Industry. In *Proceedings (online) of the 9th Workshop on Economics of Information Security*, Cambridge, MA, June 2010. http://weis2010.econinfosec.org/papers/session2/weis2010_wondracek.pdf.

[62] Jonathan Zittrain. *The Future of the Internet: And How to Stop It.* Allen Lane, London, 2008.