Discussion paper on the coverage of crime statistics

23 January 2014
Introduction

This discussion paper has been produced in response to questions about the coverage of official statistics on crime, in particular, the extent to which new forms of offence such as cyber-crime are covered in existing figures. The paper, which has been produced in consultation with the independent Crime Statistics Advisory Committee (CSAC), presents an overview of the existing coverage, discusses challenges in measuring cyber-crime, and outlines steps taken to improve measurement of cyber-crime.

The two headline measures of crime reported by ONS in the quarterly official statistics on crime (i.e. police recorded crime and the Crime Survey for England and Wales) have both pointed to a sharp reduction in crimes measured by the two series over the last 10 to 20 years.

The estimate from the Crime Survey for England and Wales (CSEW) for the year ending March 2013 showed that the volume of crime measured by the survey (8.6 million) was down 55% from the peak estimated by the 1995 survey (equivalent to 10.5 million fewer offences). The police recorded crime series cannot be reliably compared beyond 2002/03 (the last major change in recording practice) but that series shows the count of recorded crime in the year ending March 2013 was 38% lower than the volume recorded in 2002/03.

These reductions have been driven by falls in the volume of crimes of domestic burglary, vehicle-related theft (including theft of and property from vehicles) and vandalism/criminal damage. These trends in England and Wales have been mirrored in the rest of the UK and in other western democracies, such as the United States and Europe.

With the rise of new technology, and specifically the internet, new methods of committing crime have emerged. For example, the offence of fraud (i.e. false representation for personal gain) is a long established crime. However, the internet provides a new vehicle, for example to enable fraudsters to attempt scams online. Similarly, the internet provides paedophiles with a new route to engage in the sexual grooming of children and in the sharing of indecent images. At the same time, cyber-space allows the proliferation of such crimes on a large scale.

As well as providing a new method for committing established crimes, the internet provides opportunities to undertake new types of crime. Just as the offence of phone tapping could not have existed before the creation of the telephone, computer hacking could not have taken place before the rise of the internet.

A useful typology has been developed that distinguishes between cyber-enabled crime and cyber-dependent crime (McGuire and Dowling, 20131). Under this typology, cyber-enabled crime refers to using the internet as a new modus operandi to commit traditional crimes, such as fraud and sexual offences. Cyber-dependent crime is defined as using the internet to commit new types of crime not possible prior to its existence. Such crimes include illicit intrusions into computer networks (e.g. hacking) and disruption or downgrading of computer functionality and network space (e.g. using viruses and Distributed Denial of Service (DDoS) attacks). One could argue that all cyber-enabled crime is by definition cyber-dependent but the typology is helpful in unpacking

---

1 Cyber crime: A review of the evidence – Home Office Research Report 75
the term cyber-crime and in thinking about the profile of victims and offenders involved in each sub-category. In addition, blackmail using the threat of DDOS may be cyber-dependent but business disruption threats preceded the internet.

Questions have been raised about the extent to which criminality has been displaced from traditional crimes (generally well-measured by the crime statistics) into these new types of criminality (generally less well-measured by the statistics). If there has been a significant switch from traditional to new methods of crime, then the statistics could be presenting a misleading picture. There is some good evidence on the scale of plastic card fraud (much, but not all will be cyber-crime) but the true scale of cyber crime is unknown. In the absence of reliable quantitative data it is difficult to prove or disprove the claim that crime has simply been displaced into these new forms of crime.

Existing coverage of the crime statistics

The CSEW and police recorded crime provide generally good coverage of crime committed against the public, particularly for offences involving physical harm, loss or damage to property. Together they provide a more comprehensive picture than could be obtained from either series alone. However, neither the CSEW nor police recorded crime aim to provide complete counts of crime, and there are exclusions from both series.

Police recorded crime figures are supplied by the 43 territorial police forces of England and Wales, plus the British Transport Police, via the Home Office to ONS. The coverage of police recorded crime statistics is defined by the Notifiable Offence List, which includes a broad range of offences, from murder to minor criminal damage, theft and public order offences. However, there are some, mainly less serious offences, that are excluded from the recorded crime collection. These ‘non-notifiable’ crimes include many incidents that might generally be considered to be ‘anti-social behaviour’ but that may also be crimes in law (including bye-laws) such as littering, begging and drunkenness. Other non-notifiable offences include driving under the influence of alcohol, parking offences and TV licence evasion.

Police recorded crime covers people (for example, residents of institutions and tourists) and sectors (for example, commercial crime) excluded from the CSEW sample. Recorded crime has a wider coverage of offences, for example covering homicide, sexual offences, and crimes without a specific, identifiable victim (referred to as ‘Other crimes against society’) not included in the main CSEW crime count. Police recorded crime also provides good measures of well-reported and well-recorded crimes but does not cover any crimes that are not reported to or discovered by the police. The CSEW covers a narrower range of offences included in the police recorded crime collection, but reported volumes are higher as the survey is able to capture all offences experienced by those interviewed, not just those that have been reported to and recorded by the police.

The Crime Survey does not currently cover cyber-crime although attempts have been made in the past to explore elements of it through ad hoc modules of questions included in the survey from time to time. Some of these have been more successful than others but have highlighted some of the difficulties in measuring cyber-crime.
Currently the police recorded crime series will include elements of cyber-crime that have been reported to them. However, except where these are subject to a specific legal offence (such as computer misuse) they are not identifiable in the recorded crime collection. For example, cyber-bullying would be recorded under the offence of harassment and would not be separately identifiable from other offences of harassment. Similarly, sexual offences committed on-line would be hidden within the relevant offence category and would not be distinguishable from crimes committed off-line. From April 2014, police forces are being asked to flag offences that have a cyber element to gain a better understanding of the extent of cyber-crime within the recorded crime collection. Of course, the recorded crime series will never include crimes that are not reported to or not discovered by the police through proactive policing.

How much cyber-crime is there?

As is the case in relation to all crime, it is impossible to provide a definitive answer to the question of what is the volume of cyber-crime? A recent review of the evidence base (McGuire and Dowling, 2013) highlighted that industry estimates of the scale of cyber-dependent crime are massive. For example:

- Symantec reported blocking 5.5 billion ‘attacks’ and detecting 403 million unique variations of computer viruses or other malware globally in 2011;
- Symantec also reported that spam traffic, represented 69% of all emails in 2012;
- Sophos showed that the proportion of PCs experiencing a malware attack, whether successful or failed, was almost 4% over a three-month period.

However, official records of cyber-dependent crime show relatively few reports by victims of cyber-dependent crime to the authorities. For example, just 7,427 crimes and incidents of computer misuse and extortion were reported to Action Fraud (and thus, included within the official statistics on crime) during 2012. The most common incident reported was illicit distribution of viruses, spyware or other malware (3,949 reports), which accounted for over one-half of computer misuse incidents, followed by reports of individuals hacking into social media and email (1,603 reports).

Likewise, there have been relatively few prosecutions under the Computer Misuse Act (CMA) 1990, with initial proceedings taken against 101 people, and 88 people sentenced with a primary offence under the Act between 2007 and 2012 (quoted in McGuire and Dowling).

This discrepancy between the supposed threat suggested by industry figures and official crime and justice records seems slightly incongruous. In part, it might be explained by the fact that security filters have been largely effective in blocking attempts to perpetuate crime and that few members of the public actually experience such victimisation. It may also reflect that people simply delete phishing emails and view them as a nuisance rather than as an attempt to victimise them. The 2011/12 CSEW included questions on mass marketing fraud and found that while 56% of adults had received an unsolicited communication in the previous 12 months, only a very small percentage had responded to them and actually fallen victim. However, in the context of a face-to-face interview, there may be some under-reporting as respondents may feel embarrassed to admit having responded to such communication.
More generally, under-reporting of cyber-dependent crime is thought to be an issue, particularly with regard to businesses and public sector organisations that may fear commercial or reputational damage from such disclosures.

The evidence on cyber-enabled crime is similarly patchy. As with conventional crimes, acquisitive offences are likely to dominate overall volumes. So there is evidence to suggest that cyber-enabled fraud is much more prevalent than sexual offences committed on-line. For example, Action Fraud received 47,980 reports of cyber-enabled fraud (included in the official statistics on crime) during 2012, whereas the Child Exploitation and Online Protection Centre received 3,652 reports during 2009/10.

Of course, in both spheres it is likely that there is significant under-reporting of crimes. While attempts to commit crime are counted on a par with successful incidents in conventional crime statistics, it is debatable whether it makes sense to do so in the field of cyber-enabled fraud, even if it were possible to accurately do so (see below).

Industry sources show the scale of financial losses resulting from financial fraud online and retail fraud run to hundreds of millions of pounds per year. While it is not possible to translate this into crime incidents it is clear that this would represent a huge increase in the crime statistics if they were to be included. Whether or not the volumes would be large enough to more than make up for, or equal, the reduction in traditional crimes (10.5 million CSEW offences a year) is unclear. In the latest crime statistics frauds reported by Action Fraud and other industry sources account for around 500,000 offences in the last 12 months. Thus unless there is a large level of under-reporting, it seems unlikely that cyber-enabled crime is running at such high volumes to have meant the fall in crime reported by the two main measures of crime is misleading.

Challenges in measuring cyber-crime

The measurement of cyber-crime presents a number of specific challenges. Both the CSEW and PRC have a victim-focus and a key principle of counting crime is that one crime is recorded for each victim. In the CSEW, victims are households or members of those households. In the PRC series, additional victims are businesses and other organisations.

Cyber-crime can present challenges in terms of identifying and counting victims. For example, in areas such as bank and credit card (cyber-enabled) fraud, there may be ambiguity about the victim. Is it the bank or financial institution who suffers the loss, or the customer who may or may not suffer direct financial loss but certainly will suffer some inconvenience from dealing with the aftermath? Should both be counted as victims? It is difficult to think of an analogous position with conventional crime types.

A further measurement challenge presented by cyber-crime is that the internet provides the means for criminals to attempt to commit this type of crime on a grand scale. The victim-focused National Crime Recording Standard requires that an offence should be recorded for each individual victim. Thus a single act of uploading a computer virus or sending a malicious e-mail may impact on thousands of people and could (in theory) result in thousands of crimes being recorded. This presents a conceptual challenge compared with more traditional acquisitive crimes such as
domestic burglary or car theft. Even if it were possible to count accurately the number of direct and indirect victims, does it make sense to combine such counts with more traditional counts of crime?

There is an argument that, even if attempts were to be excluded from counts of cyber-crime, there may still be public interest in quantifying the scale of attempts as a measure of potential harm. For example, one could include questions on the Crime Survey asking whether respondents have ever had to disinfect their computing devices because they had a virus.

Cyber-crime is also more complex than more conventional crime in terms of jurisdiction. The ONS crime statistics aim to provide a measure of crime committed in England and Wales. Thus, a robbery experienced by a victim on holiday abroad will not appear in either the police recorded crime or CSEW series. By its nature, cyber-crime crosses geographical boundaries, and cyber-space itself is difficult to pin down to geographical territories. While it is often possible to identify where the victim or victims reside, it is often not possible to identify where the offence originated. But there is an argument that this is irrelevant from a victim-focused perspective. Centralised reporting systems (like Action Fraud) also mean that it often not possible to provide any sub-national breakdowns of the data. This raises another conceptual challenge.

**What is being done to improve measurement of cyber-crime?**

One important area of cyber-crime is fraud. There has been a significant change in the recording by the police, for statistical purposes, of fraud offences. Over the last year police forces have progressively moved to a system of recording all frauds centrally via the Action Fraud national reporting centre, and from April 1st 2013 all forces have completed this transition. Action Fraud’s role has since expanded to also be the national reporting centre for cyber-crime.

The ONS quarterly releases are showing large increases in the amount of fraud recorded by the police, for example up 27% year on year in the latest publication. There are a number of factors that may have contributed to this increase including:

- the centralisation of recording fraud and a possible improvement in recording practices resulting from having a specialist team dealing with fraud;

- an increased proportion of victims reporting fraud following publicity around the launch of Action Fraud; and,

- a possible increase in the volume of fraud.

It is not possible to separate out or quantify the scale of each possible effect. A clearer picture will emerge over the next one to two years once the new recording arrangements have matured.

Following advice received from the Crime Statistics Advisory Committee, the ONS will be conducting some work exploring the feasibility of extending the main victimisation module in the CSEW to cover elements of cyber-crime. This work includes developing and cognitively testing questions for inclusion in the survey and fieldwork piloting. It will also include examining what impact adding such questions may have on existing questionnaire length and on existing time series. This work will be extensive and is expected to run throughout most of 2014.
ONS will keep users informed of the work and welcomes views from users on the issues raised in this discussion paper. For further information contact the ONS Crime Statistics team:

Contact Name  John Flatley  
Tel:  +44 (0)207 592 8695  
Email:  crimestatistics@ons.gsi.gov.uk  
Website:  www.ons.gov.uk