Mapping and Measuring Cybercrime

Stefan Fafinski, William H. Dutton and Helen Margetts
Oxford Internet Institute
University of Oxford
June 2010

Foreword

Policing practices are often shaped by incident reports and evidence of shifting patterns of crime. This makes the collection and analysis of crime statistics of great value. Cybercrime is no exception. Statistics are being collected on cybercrime by police forces and private bodies around the world.

However, the distributed nature of the Internet makes it challenging to examine the specific geographies of cybercrime. Given the comparatively recent rise of criminal threats online, there are few agreed standards over the best ways to map and measure the nature and incidence of crimes perpetrated over the Internet. As with other crime, there can be disincentives to report cybercrime, such as fears that reports could undermine public confidence in a business enterprise, but also incentives to over report, such as to grab headlines.

This paper stems from a day-long invited forum held on 22 January 2010 that discussed the most appropriate ways of measuring and mapping cybercrime to inform legislative, research and policy debates. The forum's forty participants comprised:

- members of police forces involved in serious and technology crime policing;
- members of UK Parliament;
- representatives from leading computer security firms
- leading academics in UK and US universities involved in allied research from areas across disciplines including law, criminology, sociology, and cyber-geography

Following the invited forum, a public panel highlighted the findings of the day's discussions, particularly in relation to the most appropriate ways of mapping and measuring cybercrime to inform legislative, research and policy debates.

This discussion paper draws primarily on discussions at the invited event, the public forum, position papers and other contributions from participants in summarising the main themes and findings that emerged.

The forum was organised by the Oxford Internet Institute and was supported by a grant from Nominet UK.

Professor William H. Dutton

Director

Oxford Internet Institute

University of Oxford

Acknowledgements

The OII greatly appreciates the financial support, participation and encouragement of Nominet UK in making this event a reality. We further appreciate the early and continuing involvement and enthusiasm of the Rt. Hon. Alun Michael MP in bringing this forum to fruition. He proposed the initial idea, and advised us throughout the process.

We are of course indebted to all forum participants. Their expert, lively and questioning contributions provided a rich source for the paper, even where specific individuals could not be credited. The authors take sole responsibility for the interpretation of this material, while acknowledging the invaluable expert contribution from the many participants in helping to produce this analysis.

The Rt Hon. Alun Michael MP, Dan Mount and Ian Brown played a key role in proposing and selecting participants. Special thanks are also due to the OII events and technical teams – particularly Ida Persson, Jennifer Darnley, Linda Frankland, Tim Davies and Arthur Bullard for the smooth running of the event and to Quentin Cregan for his assistance in capturing the day's discussions.

Stefan Fafinski

Bill Dutton

Helen Margetts

Executive summary

The OII forum was organised to facilitate a dialogue between policymakers, police authorities, representatives of the computing industry and leading international academics on issues of mapping and measuring cybercrime. Its primary aims were to inform decision making in the policy area of cybercrime response and to support a more sophisticated rounded understanding of the issues involved. While the forum was not asked to reach a consensus in any area it raised a number of critical issues and points for further research. The following points summarise some of the key issues raised and associated questions from the day.

Why map and measure cybercrime?

- To inform crime reduction initiatives
- To enhance local and national responses
- To identify gaps in response
- To provide intelligence and risk assessment
- To identify preventative measures
- To facilitate reporting
- To educate and inform the public
- To identify areas for further research

Definition

- There is no set definition of cybercrime. Defining cybercrime becomes a key analytical problem.
- Segmentation of the cybercrime landscape is desirable
- A mapping exercise should be undertaken to show the geography of particular types of cybercrime, which might enable the discovery of patterns, such as overlap between areas of existing crime and cybercrime

Data

- There are several organisations involved in collecting data in this area
- Police data is under-reported and under-recorded for a variety of reasons: fear of negative publicity; lack of incentive; perception that the police response will be ineffectual; no prospect of restitutionary damages; victims not realising that they have been victimised
- Data from the industry should be viewed with caution, particularly where there is a vested interest in highlighting various products or services

- Data can suffer from methodological limitations: small sampling sizes extrapolated to huge populations; rebasing of data year-on-year
- Data could be used to produce local cybercrime maps for local law-enforcement operations

Governance

- The intervention of a global UN-style international agency would be unworkable and could potentially do more harm than good
- A liberal, co-operative governance approach could potentially achieve the desired outcomes (whether reduction of crime, nuisance, threat, harm or risk)
- The instinctive use of legislation without due consideration for alternatives is not desirable
- There are multiple agencies involved in cybercrime response which leads to a confusing administrative context: a mapping exercise could give insight into the role of the state in future cybercrime governance
- The disparate agencies involved are unsure how to proceed and are not equipped to deal nimbly with the evolving nature of cybercrime

Key questions for further consideration

- What is the purpose of the mapping and measuring exercise – to reduce incidents or to minimise harm?
- What data has to be measured – incidents, crimes, vulnerabilities, threats, harm, risk?
- How will it be measured?
- At what level should data be collected – locally, regionally, nationally or internationally?
- How should individual, national or corporate statistics be differentiated and disaggregated?
- What level of mediation is required?
- How can it be ensured that different sources are measuring like-for-like?
- How reliable is the data?
- Who is the ‘victim’ of cybercrime?
- Where do the harms lie?
- What are the preventable harms?
- Are there non-criminal harms? (‘cyberabuse’ rather than ‘cybercrime’)
- How is economic harm assessed?
- If individuals are given data on local cybercrime, or risks to their own system, what expertise and tools can be given to protect them?
- Should the geography of cybercrime be mapped?
- Should a policy mapping exercise be undertaken?

- Does cybercrime require a different approach to governance in the context of criminal justice? Could a focus on 'cybercrime' deflect attention from taking more pragmatic actions to improve the security of systems linked to the Internet?

Introduction

> … there is a clear lack of adequate statistics measuring the state of trust and security in the Information Society. Current data available is insufficient, fragmented, and often incomparable. There exists no coherent set of reliable data based on ... threats, incidents or perceptions of trust and security.
>
> Jacques Bus (cited in Galatsas 2007:2), Head of the ICT-Security Unit, European Commission

Why map and measure cybercrime?

'What is the nature and extent of cybercrime?' seems, on the face of it, to be a simple question, yet it is currently impossible to answer in terms of incidence and prevalence across populations. However, crime reduction initiatives are customarily founded upon data which can, to a reasonable degree of accuracy, depict both the types of crime that are being committed and indicate how commonplace, or otherwise, such crimes are. Similarly, one simple measure of the effectiveness of responses to crime is the extent to which crime rates have decreased, or otherwise. A set of coherent, reliable data would better inform policy approaches to cybercrime and gauge their success. It is for this primary reason that attempting to map and measure cybercrime is attractive. As Wade Baker put it 'measurement enables management' although the security community is 'prone to jump to management while bypassing measurement'.

Local crime reduction

In terms of a general high-level response to cybercrime, the Digital Britain report (Department for Culture, Media and Sport & Department for Business, Innovation and Skills 2009) welcomed proposals to 'enhance the levels of coordination between different groups and initiatives across the e-crime spectrum'. In essence, this involves a partnership approach between parliamentarians, Government and business to look across the spectrum of issues and responsibilities and to promote new efforts in the sphere of self-regulation; referred to in the report as the 'Tripartite Internet Crime and Security Initiative'. This initiative represents a partnership approach with the aim of reducing cybercrime.

In this sense, an analogy can be drawn between this proposed partnership approach and that taken at the local management level to 'traditional' crime by Community Safety Partnerships (CSPs; formerly known as Local Crime Reduction Partnerships). These CSPs involve the police, local authorities, the probation service, health authorities, the voluntary sector and local residents and businesses sharing information and working together to reduce crime and disorder in their local areas. These CPSs are under a statutory duty (under the Crime and Disorder Act 1998, s17) to do all that they reasonably can to prevent crime and disorder, anti-social behaviour, and substance misuse in their area. As well as working to reduce offending, since 1 April 2010, they also have a new statutory duty (under the

Policing and Crime Act 2009, s108) to include initiatives designed to reduce reoffending. Therefore, these CSPs must work at the local level not only to reduce crime, but also to engage with some form of rehabilitation strategy. It may be that a similar model proves to be attractive in the governance of cybercrime, where affected individuals interact with local agencies to report and receive information on threats and vulnerabilities at the same local level.

Risk, measurement and local governance

Without engaging in any depth with theoretical discourses on risk (for more detail, see Fafinski 2009: 132-178), the realist perspective draws on technical and scientific approaches to measurement and quantification, considering risk in terms of the scale of its consequences and the likelihood that the risk will occur. Here a risk is defined as the product of the probability and consequences (magnitude and severity) of an adverse event (Bradbury 1989) and requires a quantification of both the probability of the hazard and the scientific modelling of the magnitude and severity of the consequences should they occur. Thus as Brown (1989: 2) suggests, the primary objective of such a techno-scientific approach to risk is that objective measurement will facilitate understanding and will 'provide a route out of the ever-growing bitterness of clashes between affected publics and the managing institutions'.

From this standpoint, CSPs, as governance networks (Rhodes 1997; Rosenau 1995), rely upon information to drive local strategy and maximises the prospect of effective crime prevention: the results of which can then be shared with the public by way of self-validation. CSPs measure the levels of crime and disorder problems in their areas and consult widely with the community in that area to ensure that the partnership's perception, based on data, matches the subjective viewpoint of the local populace, particularly with minority groups such as the LBGT (lesbian, bisexual, gay and transgender) community, or members of ethnic or religious minorities. Once levels of crime are measured, then the partnership devises its strategy and its measures for tackling the priority areas identified via the data. The strategy will include both targets and 'target owners' for each priority area and its execution is kept under review by the partnership as the targets are measured and re-evaluated in the light of new data.

CSPs, then, are founded on a clinical audit of what criminal activity is actually happening, measured as accurately as possible. This, then, is not just measurement for its own sake, but measurement with a purpose which identifies and prioritises key issues objectively, rather than pursuing subjectively-perceived 'popular causes'. Measurement must therefore be as valid and reliable as possible, such that it can effectively assess risk and thereby inform public policy and practice.

If a CSP-style networked crime reduction model is to be applied to cybercrime, then effective mapping and measuring is essential. This is relatively easy for CSPs: the crimes with which they are concerned are committed locally and managed by a criminal justice system that is familiar with those traditional offences. In the cybercrime world, crimes may be initiated from anywhere in the world with network connectivity and their comparative novelty presents other challenges of measurement. The response to any new cybercrime data is, at present, reactive rather than proactive. There is limited informed, reflexive strategy. Therefore, in order to create a new methodology and a strategy to reduce cybercrime, upon which public priorities and policies must be set, it is necessary to consider two key points:

- What has to be measured? and, only then:
- How will it be measured?

The purpose of this forum was to begin an exploration of the problems involved in addressing these deceptively simple-looking questions.

Structure of this paper

This paper begins to address the issues that arose from the forum discussions. The day itself was structured into four discussion areas, namely:

- The vision: mapping and measuring cybercrime
- Technical feasibility: conceptual, methodological and technical approaches
- Ethical, legal, and institutional challenges
- Key issues and recommendations and next steps.

However, the debates surrounding each of these areas raised cross-cutting issues that focused on three broad topics:

- **Definition**: matters of terminology, taxonomy and segmentation
- **Data**: availability, reliability and validity of sources
- **Governance**: approaches to governance and policy

This paper will adopt these three broad themes and encapsulate, as far as possible, the forum contributions in each area respectively. The conclusion provides an overview of the most pressing questions that present future opportunities for research in this area and the challenges in attempting to map and measure cybercrime.

Definition

> There is, as we have already noted, no legal definition of 'e-crime' nor are data on the incidence, investigation or prosecution of e-crimes (that is to say, crimes committed by means of or with the assistance of the use of electronic networks) collected.
>
> House of Lords Science and Technology Committee (2007: 64)

What is 'cybercrime'?

Cybercrime is not a legal term of art. As such, it carries with it a certain degree of contextual mutability, including 'cyberspace' crime (Gibson 1982, 1984) and 'the transformation of criminal or harmful behaviour by networked technology' (Wall 2007: 10). Cybercrime can therefore encompass the use of computers to assist 'traditional' offending, either within particular systems or across global networks. It can also include crimes that are wholly mediated by technology – so-called 'third generation' cybercrimes (Wall 2007: 10). Such cybercrimes, such as spam e-mail for example, are solely the product of the Internet and could not exist without it. However, many of the so-called cybercrimes that have caused concern over the past decade are not necessarily crimes within the meaning of the criminal law. In essence, the suffix of 'crime' is attached to behaviours which do not readily fall within the boundaries of the criminal law. There is, therefore, not always a legal basis for certain

so-called cybercrimes. These include the more controversial harms which fall outside the jurisdiction and experience of the criminal justice process including cyber-rape (MacKinnon 1997) and the vandalism of virtual worlds (Williams 2006).

There is, therefore, a considerable linguistic agency associated with the term cybercrime, particularly the use of the word 'crime' in relation to something which might not lie entirely within the boundaries of the criminal law. As Nimmer (1985: 9) helpfully summarises:

> Although aspects of computer use in society create vulnerabilities or opportunities for abuse these are not always qualitatively different from vulnerabilities that exist independently of computers. In many cases, however, the degree of risk and the nature of conduct are sufficiently different to raise questions about basic social decisions concerning levels of criminality for computer-related actions and the ability to discover and prosecute them under current law. Whether these are discussed under the heading of computer crime or merely as general criminal law problems is not important.

David Bray illustrated the definitional difficulties by asking whether the definition of cybercrime should include only crimes for economic gain (such as fraud, identity theft or blackmail) or whether it should include cyber espionage by non-state actors or cyberterrorism: is cutting an undersea data cable a cybercrime? Does it depend on who did the action and to whom the action was aimed?

Taxonomies of cybercrime

Discussions of cybercrime taxonomies gave rise to two schools of thought. First, that cybercrime could be broadly categorised in some way. For example:

- Traditional crime that **affects** technology (such as stealing a computer)
- Traditional crime that is **mediated** through technology (such as 419 fraud or distribution of obscene content)
- **Exclusively** technological crimes (such as distributed denial-of-service attacks).

Sarah Oates described this as:

- Virtual crime
- Hybrid crime
- Augmented traditional crime

This tripartite split was expressed in an alternative form as:

- Crimes **against the machine** (such as unauthorised access)
- Crimes **in the machine** (such as storage of child exploitation images)
- Crimes **via the machine** (such as email or web mediated fraud).

Similarly, the Council of Europe Convention on Cybercrime (2001) offers a categorisation of offences as follows (see Appendix 2)

- Offences against the confidentiality, integrity and availability of computer data and systems
- Computer-related offences

- Content-related offences

Alternatively, Peter Sommer put forward the position that attempting to establish a taxonomy of cybercrime is an artificial and somewhat pointless exercise: that crime is conduct that is outside the boundaries of the criminal law and that the means of commission or target are immaterial. This echoes the view of Ingraham (1980: 438) put forward thirty years ago, when the first debates about the meaning of computer crime were emerging:

> Striking a watchman with a disk pack should remain the battery that it is, and not be elevated to the status of a computer crime. There are enough red herrings in our courts already.

Analogical pitfalls

There is a difficulty in trying to draw any complete analogy between the online and offline worlds. The mid-1990s debates between Easterbrook and Lessig on the meaning of 'cyberlaw' illustrate the problem. For Easterbrook, a taxonomy of 'horse law' would be flawed, because:

> ...the best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on 'The Law of the Horse' is doomed to be shallow and to miss unifying principles (Easterbrook 1996: 207)

However, Lessig (1999) argued that legal perceptions and rules would need to evolve as the cyberspace environment developed and expanded and that a new conceptualisation of cyberlaw would be required. By extension, this would also necessitate a redefinition of cybercrime as a subset of cyberlaw.

Within the forum, the difficulty of analogy was illustrated by reference to 'car crime': a term which could encompass parking, speeding, careless driving, frauds committed by garages who overcharge, use of the car as a getaway vehicle, the car as a scene of rape, the car as a murder weapon and so forth. It was argued that the car transformed traditional crime. Burglars, for instance, were no longer restricted solely to their own geographical area; the locus of their criminal activity being extended. Burglary 'away days' from home to an appropriate target location were facilitated by the availability of accessible personal transport.

The Internet has transformed traditional crime on a global scale. The analogy was continued: Bonnie and Clyde stole cars and crossed state lines to commit robbery. The US legislature responded by making car theft and robbery federal offences, thus increasing the odds of arrest.

In a similar way, the Cybercrime Convention (see Appendix 2) provides a framework for international co-operation in this field, creating a quasi-federated response. It sets out such procedural law issues including the expedited preservation of stored data, the expedited preservation and partial disclosure of traffic data, production orders, search and seizure of computer data, real-time collection of traffic data, and interception of content data. In addition, the Convention contains a provision on a specific type of trans-border access to stored computer data.

However, the question is then raised as to whether there is an adequate set up of international investigation and policing to operate within this legislative framework. In the car crime example, the US response did not go beyond (challenge) national sovereignty, yet international cooperation, which is central to the Cybercrime Convention, raises major issues between signatories.

Defining cybercrime is therefore a key analytical problem.

What next?

Although there was some disagreement on the details, forum participants were generally agreed that it would be desirable:

- to start segmenting the cybercrime landscape
- to produce a conceptual map showing the overlap (or otherwise) between areas of existing crime and cybercrime, and
- to explore the feasibility of mapping the geography of particular types of cybercrimes.

These are two different, but complementary, uses of the concept of mapping: one conceptual and one geographic.

Data

Having established that the first stage in the process is producing a cybercrime map, the next must be in populating that map with data: there is no practical benefit in having a map without data.

There are many sources of statistics: the questions then become:

- how should individual, national or corporate statistics be differentiated and disaggregated?
- what level of mediation is required?
- how can it be ensured that different sources are measuring like-for-like?
- how reliable is the data?

Sources of data

The number of organisations whose activities centre around cybercrime is vast even when the UK is considered in isolation from other countries. A map of the Information Assurance Community within the UK (EURIM, 2008) identifies many organizations involved in collecting information on cybercrime, including over 30 Trade Association and Industry groups; 11 government departments running nearly 30 programmes or information exchange groups, and 12 professional bodies themselves split into further specialist working groups, not to mention the police, academic experts, international forums and government/ industry collaborations.

The problems of under-recording and under- and over-reporting

Data collected by the police suffer from under-reporting and under-recording, from both the public and from businesses. The original source of UK law enforcement expertise on cybercrime was the National High-Tech Crime Unit (NHCTU), established in 2001 as part of the National Crime Squad, a unit dedicated to tackling cross-county and international crimes (Valeri et al. 2006). NHCTU established a confidential reporting charter where companies or individuals reporting cybercrime could do so anonymously. More recently the National Crime Squad has merged with the National Criminal Intelligence Service or NCIS, and with aspects of Customs and Excise, to create the Serious Organised Crime Agency (SOCA). As part of this reform the NHTCU has been amalgamated into the cybercrime unit of SOCA, which has subsequently dropped the NHTCU's confidentiality charter. This is likely to result in fewer reports to police (Bennett 2006).

Businesses rarely report incidents due to a fear of negative publicity. On the basis of one estimate, a fear of damage to reputation lead to 97 percent of the worst incidents experienced by UK businesses in 2007 being kept 'in house', that is, knowledge of the incident was contained within the organisation (BERR 2008: 31). Fear of damage to reputation is repeatedly cited as a key reason for not reporting incidents to the police by UK businesses (BERR 2008). Richardson's (2007) annual Computer Crime and Security Survey in the USA has also consistently shown that negative publicity is the main reason businesses would not report incidents to law enforcement:

> If someone got into our data, the last thing we'd want is for it to be all over the courts and the papers. Software is our business. Do you really think we'd want our customers to hear we'd been caught out? That would be commercial suicide. (Fafinski, 2009: 51).

Similarly, the incentives to report instances of data breaches to customers are in favour of secrecy:

> A company whose systems have been compromised has every incentive to keep quiet about it, and will probably receive legal advice against notifying affected individuals … Thus security breaches affecting the individual are typically detected when the individual complains of fraud. Such complaints are often met with hostility or denial by financial institutions or with a demand that the customer explain how the dispute might have arisen" (FIPR cited in House of Lords 2007: 210).

A further cause of under reporting to the police by organisations appears to be that the police are not viewed as experts in the arena of information security (Wall 2007). Only eight percent of respondents to the UK 2008 ISBS (the 2008 BERR survey) had approached the police for guidance or expertise on information security, whereas personal contacts within the business or security industry were consulted by 39 percent of respondents (BERR 2008: 10). Even when an incident is reported to the police, there might well be an absence of technical understanding about what the offence is, and therefore what it might signify, as well as a shortage of the technical resources to address it. David Ransom commented that there was an urgent need to train the police service in cyber security. While there are a few IT forensic experts within the police, the general population of police 'first responders' is ill-equipped to deal with the problem. Such views were echoed in interviews with both police officers and technology users alike (Bennet 2006; Fafinski 2009: 51):

> …directing firms to local police stations to report a computer crime is a big backward step…can you imagine trying to explain to your local bobby that you have been under a 20 million packets per second DP [or] SYN flood all weekend? He'd probably tell you to call the water board.

> If someone came up to my desk and told me that they had a virus, I'd tell them to go to their doctor. It would be different if they'd had their car nicked, I suppose, but we can't go looking for things that don't exist, can we?
>
> We just haven't got the time. We can't handle burglaries, let alone all these computer attacks. I'm not saying that we shouldn't. We just can't.
>
> What would be the point in going to the police? They're not going to recover our data. Even if there's a miracle and they do catch whoever's done it, we'll still be out of pocket. Locking someone up won't help us.

One contributing factor to under-reporting raised by the last comment may be that there is no prospect of restitutionary damages or compensation for loss in a criminal prosecution.

Under reporting to the police is not restricted to organisations. According to the British Crime Survey (2004), only 13 percent of households whose Internet security had been breached reported the incident to anyone. A third of these reported the incident to a website administrator and 27 percent to an Internet Service Provider (ISP). The proportion reporting hacking attacks to the police is not mentioned, presumably because the figure is so low. Similarly, whereas 37 percent of households experiencing computer viruses reported the virus incident to anyone, 9 percent had reported the virus to their ISP, six percent to a website administrator, but only one percent to the police. Even information breaches which lead to monetary loss, or posed the threat of this, were reported in low proportions: over three quarters of those who reported a credit or debit card fraud in the Offending Crime and Justice Survey (2004) reported the fraud to their credit card company or bank, where as only a quarter reported their experience to the police (Wilson et al. 2006). Jan Sponle suggested that other reasons for not reporting cybercrime is simple embarrassment at being victimised.

Cybercrimes reported in isolation will be assumed to be single and unrelated incidents until the police are able to farm the data for links between seemingly disparate events. The current police recording system does not allow aggregation of single incidents in order to reveal underlying patterns and trends: the bigger picture (Wall, 2007). An isolated denial-of-service attack reported by a home user might not appear serious (or expensive) enough to warrant attention by the local police force, and will definitely not be passed up to national coordinated centres such as the SOCA e-crime unit. However, if these data were aggregated, a coordinated (automated) attack might be revealed. Therefore offences classed as level 1 and level 2 on the UK's National Intelligence Model are 'slipping through the net' (House of Lords 165: 68).

Cybercrime surveys

There are currently no methodologically sound international surveys which measure cybercrimes suffered by businesses or home users (Galetsas 2007; Wall 2008). The only exception to this is the ICVS (International Crime Victimisation Survey), which asks respondents about 'consumer fraud'. Even here the numbers of victims are small and susceptible to underreporting, particularly if individuals are unaware they have been victims of fraud (van Dijk et al. 2008).

Within the UK, the British Crime Survey (BCS) and the Offending Crime and Justice Survey (OCJS) ask individuals about some aspects of computer crime, and theft of computer-related equipment. A representative sample of UK businesses are asked about their experiences of computer crimes every two years in the Information Security Breaches Survey conducted by PricewaterhouseCoopers on behalf of BERR (previously the Department of Trade and Industry) (BERR, 2008). Together the BCS, OCJS and BERR combine to give a mosaic of

information relating to UK cyber-victimisation. However, the lack of awareness of being a victim of cybercrime leads these sorts of victim-reporting surveys to underestimate incidence and prevalence rates. End-users often need assistance in determining whether they have been a victim of a cybercrime and, if so, which one. It was noted that victims may claim to 'have had their email hacked' whereas, in actual fact, they were the subject of a phishing attack. These kinds of issues highlight the methodological problems in victim surveys: victims are often insufficiently expert enough to understand what has happened to them. This is not the case in the offline world: with homicide there is usually a body, people know how to report it and people know that they should. However, with cybercrime, there is often no 'body'. Victims may not know that they have been attacked, or if they do, they may not know where to report it to or even what to report. Ken Rabey commented that more needs to be done on public perceptions of e-crime. Awareness amongst businesses about various security breaches also appears to differ according to the detection software and reporting procedures they have in place (BERR, 2008). At the very least, though, as Mike Levi commented, crime surveys, at the very least, are good heuristic devices for stimulating prevention awareness in particular sectors.

In the instance of computer and Internet-facilitated crimes such as phishing, and the installation of malware, data collected from specialist security software vendors are all that is available (Wall, 2008). These sources also suffer from a variety of methodological issues. They are however suitable in some instances for assessing changes in the *modus operandi* of criminals, the behaviour of end-users and for rough tracking of certain overall trends. However, as Ana Canhoto commented, the relationship between patterns of data and underlying criminal behaviour is often based on assumptions and speculation about the intention of the perpetrators, and the conceptualisation of those data patterns is further influenced by contextual factors which introduce further subjectivity into the task.

Conflicts of interest

There are, however, potential conflicts of interest: the inexact science of cybercrime estimation is particularly prone to bias and error when carried out by companies with a vested interest in highlighting the need for their various products and services (Wall, 2007: ch 2; Newman & Clarke 2003). Therefore although such reports provide exciting headlines for newspapers, they must be interpreted with caution.

Wall (2007) describes a specific example of the apparent bias in data produced by vendors with such a vested interest. In October 2005, John Leyden, a journalist from *The Register,* investigated claims by an anti-spyware firm about the levels of infections caused by spyware. Leyden revealed that the infection rates had been calculated by counting benign 'cookies' along with the more malicious software such as Trojans and keyloggers. Disaggregation of the benign software cookies from the malicious decreased the number of infections on each PC from 18 to 4.5. However, to imply that all results are biased or skewed is to do a disservice to the many professionals working within information security research. The intention here is not to imply deliberate misrepresentation, but rather to point out the methodological issues which need to be addressed if genuinely reliable statistics are to be produced and accepted by both academics and practitioners.

Methodology issues

In addition to possible bias, methodological shortcomings plague many of the published statistics. Well intentioned surveys of businesses provide little useful information if non-representative samples are used. Richard Clayton commented that the way in which crime and criminal activity are counted (i.e. the methodology used) can prejudge policy responses

by deciding what is going to be measured: since it is those measurements that will be used to judge whether or not a response is effective.

Ryan and Jefferson (2003) specifically analysed the different prevalence rates across several surveys asking similar questions to different convenience samples, and clearly demonstrated the wide range in results. Therefore, such surveys at the best can indicate overall trends in numbers of incidents if their convenience sample is relatively stable over time.

Language and rhetoric

A more subtle and powerful factor which skews the perception and measurement of cybercrime is that of language and logic. The rhetoric of journalism, for example, often leads to the over-dramatisation of crime, which can cultivate a perception of a more dangerous Wild West of the Internet than is actually the case. The language used by private companies especially is often both emotive and invites inductive reasoning to equate tools and opportunities for crime to be equated to crime rates. Given such emotive presentation perhaps it is not altogether surprising that the media often interprets a reported trend in opportunities or tools as a trend in offences or outcomes (Wall, 2007, 2008). However this interpretation has no place in accurate criminological mapping of the issue of cybercrime. As David Wall commented, ten years ago, it was perfectly possible for thieves to use coat hangers to break into cars. That is not to say that it was reasonable to then extrapolate that the billions of coat hangers in the UK represented a significant risk of car crime, although car locks have changed to make it more difficult to open a latch with a coat hanger. Thus, to equate tools or opportunities with criminal outcomes is illogical and not behaviourally defensible. Furthermore it shows ignorance of the need for the convergence of an offender or tool with a victim or vulnerable target in order for a crime to occur. For example, if cybercrime is not studied systematically and the elements which converge unpicked and quantified, opportunities for preventive measures will be missed.

Similarly, Bill Dutton gave the example of the use of the word ‘piracy’, comparing its use in terms of sharing of copyrighted material versus attacking and robbing ships at sea. While the use of ‘piracy’ is a useful rhetorical device for proponents of copyright protection, it is misleading in terms of law enforcement and public policy.

Industry reporting

For some types of crime, specialist industry niches have provided reasonably valid data. For instance, AEPOC (the European Association for the Protection of Encrypted Works and Services) is the body of expertise on issues associated with piracy of pay-TV and other digital service. The UK Payments Association (formerly APACS) and other sources continue to publish statistics estimating UK financial losses attributed to fraud. However, even data produced by specialist organisations has limitations, particularly where changes in sampling size or strategy over time leave both numbers and trends incomparable. Colin Whittaker suggested that such targeted measurements of cybercrime are likely to be most cost justified and cost effective within an industry vertical.

Academic research

Academic literature within the arena of Computer Science or Information Security only has greater value if something new is presented, such as a new protocol, piece of code or algorithm, and so it tends to be technical in nature. The focus is not on estimating overall

levels of incidents or threats. Newman and Clarke (2003) conclude that most articles on computer crime are descriptive in nature, and present estimates of various e-commerce crimes with a dose of caution. Exceptions are Jerin and Dolinsky (2001) who sampled people from the online dating community to estimate victimisation rates, and Mann and Sutton (1998) who systematically studied the illegal activities and links of two Internet newsgroups.

What to measure?

One of the key debates of the day between participants was concern with what could realistically be gained from an exercise in statistical collection and analysis. Views ranged from urging that the collection of global statistics made 'no sense at all' as the figures would be 'meaningless' on one end, to such figures being necessary to conduct any form of clinical audit and so as to establish a baseline and to understand the effectiveness of any approach, on the other. There was further debate as to whether data should be collected to measure actual crimes, incidents, harm or vulnerabilities.

Measuring harm

There seemed to be broad consensus that counting cybercrime should involve counting what has actually occurred rather than what might or could occur: crime which causes real harm to real people or institutions. However, given that not all incidents give rise to criminal liability but yet might still cause harm, then the question becomes whether counting should include harm-causing incidents which may not be crimes as defined by the criminal law itself – sometimes called 'sub-crimes'. Of course, measuring harm would then require agreement on the manifestations of harm, which would constitute an incident for the purposes of measurement. As Neil Long commented, the measurement of harm also raises other questions:

- Who is the victim?
- Where do the harms lie?
- What are the preventable harms?
- Are there non-criminal harms? ('cyberabuse' rather than 'cybercrime')
- Is the surveillance involved in tracking some activities an illegal invasion of privacy?

Martin Innes further commented that, in the current economic climate, cybercrime is just one of a range of social problems that are jostling for attention and that there are insufficient resources available to deal with everything: therefore the focus must be on activity which causes the most harm. Jennifer Perry also commented that the important thing to know was the story behind why the data collection was required at all – with the focus on the victim.

Measuring loss

Loss is a particularly common component of cybercrime harm: how should such fiscal harm be assessed and recorded in cash terms? The discussion ultimately appeared to result in a simple agreement: it would be incredibly difficult to achieve, coding it correctly would be near impossible and the figures would be likely be meaningless. Although quantifying harm in economic terms is useful in attracting policymaking attention, correctly coding and assessing particular losses would either require an extensive framework or substantial effort when acquiring data. Moreover, per incident reporting figures of loss can be wildly skewed by a

few entries. For example, a virus infection could wipe out the primary systems of a company and cause that business to shut down, laying off all employees. This would lead to a substantial financial loss. It is difficult to decide at what point to draw the line in respect of consequential losses. Guidelines as to remoteness of damage, a concept used to limit quantum of damages in, for instance, breaches of contract and negligence actions would be required. Equally, online fraud figures can often be difficult as they include everything from £5 eBay frauds to highly complex multi-million-pound carousel frauds.

To complicate matters further, a single incident may lead to different harms, which, in turn, adds complexity to any harm mapping exercise. However, although prevention from harm is a key operational objective of effective policing, there is still an element to which that which is easily measured gets enforced. Policing targets reflect such goals as a percentage reduction in, say, graffiti or parking offenders, which are readily demonstrable and as a result will decrease certain types of harm within a particular locality. Police need statistics to operationalise their strategy, particularly in the allocation of resources. However, cybercrime policing is currently reactive and intelligence-led via targeted investigation: a mapping and measuring exercise could feed into that intelligence.

What next?

The purpose of the forum was to examine the value and feasibility of a more concerted effort to map and measure cybercrime. This raised questions about the purpose of the mapping and measuring exercise. Is it to deter (that is, to minimise the number of incidents) then it should focus on the segmentation of forms of conduct; if it is to minimise the harm caused, then measurement of harm is required. The purpose will also have a bearing on the resultant policy considerations. Deterrence may be achieved by policing and a demonstration to the public that (at least some) cybercrimes are investigated and prosecuted vigorously, in a similar way to, for example, high profile drink-driving campaigns. Harm reduction could be achieved by alternative means: for instance by increased and enhanced consumer protection laws, or by improved practices on the part of consumers.

A further question that drives both policy and data analysis is at what level data should be collected, be it locally, regionally, nationally or internationally. If data is to be collected at all, then what should be done to incentivise the reporting of cybercrime? At present there are very few incentives to reporting: introduction of appropriate and suitable incentives for individuals, small and large businesses could help to address the under-reporting problem. Spencer Chainey commented that physical crime has an inherently geographic quality and is not randomly distributed and that the same principles apply to mapping crime in cyberspace, even though the criminal interaction is not a physical one. Criminal occurrences happen where ‘offender awareness space’ and opportunities coincide.

Aggregated data at the local level could also support public crime maps which, in turn, could raise awareness of cybercrimes and empower individuals to take appropriate steps towards their own safety. The questions this raises are:

- If individuals are given data on cybercrime in their locality, then what tools can be given to them to protect themselves?
- If this approach is desirable, then should any mapping exercise include a geography of victimisation?
- Is a geography of cybercrime more important for law-enforcement operations?

At the individual level, there have been efforts, such as StopBadware, to help users identify risks to the security of their systems, such as suspect software they might be asked to

download. In some respects, helping users to identify risks could be a step towards preventing crime without focusing on law enforcement per se – that is, cybercrime. Vint Cerf (2010), one of the Fathers of the Internet, suggested that it might be useful to avoid terms like cyberwarfare and cybercrime and move closer to analogies with the fire services. When a person's house is on fire, fire fighters help to put it out. They even have the right to enter the household, to identify fire hazards and have them corrected. He illustrates that with a slight shift of language, it would be possible to approach security risks in a new and possibly more effective way than in an over-reliance on crime and the police.

Levels of governance

What is governance?

In the context of this discussion paper, governance is a means of regulating relationships in complex systems (Rhodes 1994) and can be expressed as a 'function that can be performed by a wide variety of public and private, state and non-state, national and international, institutions and practices' (Hirst & Thompson 1995: 422). Inherent in these definitions is a recognition of something broader than government which includes informal as well as formal rules, described by Kjaer (2004: 4) as 'networks of trust and reciprocity crossing the state-society divide'. State and society are bonded together in the process of creating governance (Pierre & Peters 2000) and, indeed, the notion of a governance approach to controlling the misuse of technology has been mooted for some time:

> Taken together, badly designed technology, misused technology and unmastered technology concur to put society in a position where it can no longer aspire to regulating and controlling all details through its political institutions. Well-regulated sectors will co-exist with others from where we may expect influences which trigger the emergence of new types of individual and collective behaviour (Lenk 1997 cited in Loader 1997: 134).

A governance response to cybercrime requires some form of quantitative information as well as a more subjective instinct as to the current state of the cybercrime landscape. It requires a careful consideration of the extent to which data is available, the quality of that data and the use to which that data is put.

International agency is not desirable

It was suggested that some sort of bureaucratic international agency would be unworkable and could potentially do more harm than good. This is in line with a UN Congress press release (2005) which concluded:

> While there was a wide consensus on the need for a combined approach and better mechanisms of international cooperation, participants felt that a United Nations Convention on Cybercrime would be premature at this stage and that it was more critical to provide technical assistance to Member States in order to provide a level playing field.

Co-operative governance as a response

If the central agency approach is undesirable, then the challenge becomes one of formulating a better way and establishing whether a liberal, co-operative governance approach can achieve the desired outcomes (whether they are phrased in terms of reduction of crime, nuisance, threat, harm or risk). Such regulatory responses would combine nodes of both legal and extra-legal governance and facilitate the reflexive and cohesive approach to regulating cybercrime necessary in global networked society (Fafinski 2009). That said, the consensus was that unless a suitable public-private partnership was formed and started to bear fruit soon, then the government would be compelled to take a more active, interventionist role in the area whilst remembering that government must be part of the solution, but not the solution. It is a partner.

Legislation as a response

The forum also considered the use of legislation as an intervention strategy. The UK is often quick to criminalise any perceived social problem without exploration of viable alternatives. For example, the UK quickly extended the use of banning orders in response to football violence overseas and criminalised the ownership of dangerous dogs via the Dangerous Dogs Act 1991 in response to a spate of vicious attacks on young children. The problem, however, lay in defining what it called 'the type of dog known as the pit bull' which gave rise to a number of odd cases and much unfavourable public reaction to the Act. As the Rt Hon Alun Michael MP commented: 'the last thing we want is a Dangerous Computers Act'.

Finally, the multiple agencies involved in responding to cybercrime are themselves unsure as to how to proceed, facing difficulties in responding to the speed of technological development, the speed with which new cybercrimes come into being and the international trans-jurisdictional nature of the problem. The question was therefore raised as to whether a policy map in this area is desirable. The multiple agencies involved gives rise to a confusing administrative context and a mapping exercise could give an insight into how the role of the state should be designed for the future of cybercrime governance.

What next?

The next steps are to deepen the analysis of this area. A number of participants at the forum endorsed efforts to undertake a scoping study of the mapping and measuring exercise, which has since been pursued. Advances in this area could inform policy and practice in major ways.

Bibliography

Bennett, M. (2006) 'British FBI drops Confidentiality Charter for IT crime victims'. *IT Week.* [Online] http://www.computing.co.uk/itweek/news/2153704/british-fbi-drops

BERR (2008) *Information Breaches Security Survey 2008: Technical Report.* London: Department of Trade and Industry.

Bradbury, J. (1989) 'The policy implications of differing concepts of risk' 14 *Science, Technology and Human Values* 380.

Brown, J. (ed.) (1989) *Environmental Threats: Perception, Analysis and Management.* London: Belhaven Press.

Cerf, V. (2010), Keynote for the Workshop on Legal Aspects of Internet Governance at the Internet Governance Forum, Vilnius, Lithuania, 15 September.

CPP (2010) 'Millions snared in web fraud' [Online] http://www.cpp.co.uk/news/miilions_snared_in_web_fraud/

Department for Culture, Media and Sport and Department for Business, Innovation and Skills (2009) *Digital Britain: Final Report*. Cm 7650. London: OPSI.

Easterbrook, F.H. (1996) 'Cyberspace and the law of the horse' *University of Chicago Legal Forum* 207.

EURIM (2008) 'Information Assurance Community Map' [Online] http://eurim.org.uk/activities/e-crime/IA_UK_Community_Map.pdf

Fafinski, S. (2009) *Computer Misuse: Response, Regulation and the Law.* Cullompton: Willan.

Galetsas, A. (2007) *Statistical Information on Network Security*. European Commission Information Society and Media Directorate-General. Brussels: European Commission.

Gibson, W. (1982) 'Burning chrome' *Omni Magazine*.

Gibson, W. (1984) *Neuromancer*. London: Harper Collins.

Hirst, P. and Thompson, G. (1995) 'Globalisation and the future of the nation state' 24 *Economy and Society* 408.

House of Lords Science and Technology Committee (2007) *Personal Internet Security*. 5th Report of Session 2006-2007. Volume I: Report. London: The Stationary Office.

Ingraham, D. (1980) 'On charging computer crime' 2 *Computer and Law Journal* 429.

Jerin, R. and Dolinsky, B. (2001) 'You've Got Mail! You Don't Want It: Cyber-Victimization and On-Line Dating'. 9 *Journal of Criminal Justice and Popular Culture* 15.

Kjaer, A.M. (2004) *Governance*. Cambridge: Polity Press.

Lessig, L. (1999) 'The law of the horse: what cyberlaw might teach' 113 *Harvard Law Review* 501.

Levi, M., Burrows, J., Fleming, M. and Hopkins, M. (2007) *The Nature, Extent and Economic Impact of Fraud in the UK*. Report for the Association of Chief Police Officers' Economic Crime Portfolio.

Lewis, B.C. (2004) 'Prevention of computer crime amidst international anarchy' 41 *American Criminal Law Review* 1353.

Loader, B. (ed.) (1997) *The Governance of Cyberspace*. London: Routledge.

MacKinnon, R. (1997) 'Virtual rape' 2(4) *Journal of Computer Mediated Communication.* [Online] http://jcmc.indiana.edu/vol2/issue4/mackinnon.html

Mann, D. and Sutton, M. (1998) 'Netcrime: more change in the organization of thieving'. 38(2) *British Journal of Criminology* 201.

Newman, G. and Clarke, R.V. (2003) *Superhighway Robbery: Preventing e-commerce crime*. Cullompton: Willan.

Nimmer, R, (1985) *The Law of Computer Technology*. New York: Wiley.

Pierre, J. and Peters, B.G. (2000) *Governance, Politics and the State*. Basingstoke: Macmillan.

Rhodes, R.A.W. (1994) 'The hollowing out of the state: the changing nature of the public service in Britain'. 65 *Political Quarterly* 138.

Rhodes, R.A.W. (1997) *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability.* Buckingham: Open University Press.

Richardson, R. (2007) *The CSI Computer Crime and Security Survey.* [Online] http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

Rosenau, J.N. (1995) 'Governance in the twenty-first century' 1 *Global Governance* 13.

Ryan, J.J.C.H. and Jefferson, T. (2003) *The Use, Misuse and Abuse of Statistics in Information Security Research*. Proceedings of the 23rd ASEM National Conference. ASEM 15-18 October 2003.

United Nations (2005) '"Around the clock" capability need to successfully fight cybercrime, workshop told'. UN Doc SOC/CP/334.

Valeri, L., Somers, G., Robinson, N., Graux, H., and Dumortier, J. (2006) *Handbook of Legal Procedures of Computer and Network Misuse in European Countries: Technical Report*. Prepared for the European Commission. Brussels: Rand Europe.

van Dijk, J., van Kesteren, J. and Smit, P. (2008) *Criminal Victimisation in International Perspective: Key findings from the 2004-2005 ICVS and EU ICS.* The Hague: Boom Legal Publishers.

Wall, D.S. (2007) *Cybercrime: The Transformation of Technology in the Networked Age*. Cambridge: Polity Press.

Wall, D.S. (2008) 'Cybercrime, media and insecurity: the shaping of public perceptions of cybercrime' 22(1) *International Review of Law, Computers and Technology* 45.

Williams, M. (2006) *Virtually Criminal*. Abingdon: Routledge.

Wilson, D., Patterson, A., Powell, G. and Hembury, R. (2006) *Fraud and Technology Crimes. Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative sources.* London: Home Office.

Appendix 1. Forum participants

The following participants attended the OII Mapping and Measuring Cybercrime Forum on 22 January 2010. Job titles and affiliations are as they were at the time of the Forum.

Richard Allan, Facebook

Ross Anderson, University of Cambridge

Wade Baker, Verizon Risk Intelligence

Martin Boyle, Nominet

David Bray, Science and Technology Policy Institute; Institute for Defense Analyses in D.C

Sean Byrne, National Policing Improvement Agency

Ana Canhoto, Henley Business School

David Clarke, City of London Police, National Fraud Programme

Richard Clayton, Cambridge University

Quentin Cregan, Oxford Internet Institute

Susan Daley, Symantec

William Dutton, Oxford Internet Institute

Stefan Fafinski, Brunel University

Marc Goodman, Cybercrime Research Institute

Mark Graham, Oxford Internet Institute

Louise Guthrie, Oxford Internet Institute

Stephen Harrison, National Fraud Authority

Stuart Hyde, Cumbria Police; e-Crime Prevention; Society for the Policing of Cyberspace

Martin Innes, University of Cardiff

Richard Jones, University of Edinburgh

James Kemp, Nominet Trust

Michael Levi, Cardiff University

Neil Long Team, Cymru

Helen Margetts, Oxford Internet Institute

Charlie McMurdi, Metropolitan Police, New Scotland Yard

Alun Michael, Labour and Co-operative Party MP for Cardiff South and Penarth

Daniel Mount, Senior Researcher to Alun Michael MP

Sarah Oates, University of Glasgow

Tony Osborn, Symantec

Roland Perry, RIPE NCC; e-victims.org

Jennifer Perry, RIPE NCC; e-victims.org

Ken Rabey, Wolverhampton University

David Ransom, People United Against Crime

Robert Richardson, Computer Security Institute

Peter Sommer, The London School of Economics and Political Science

Jan Spoenle, Max-Planck Institute for Foreign and International Criminal Law

David Wall, University of Leeds

Jonathan Welfare, Nominet Trust

Colin Whittaker, UK Payments Administration

Yorick Wilks, Oxford Internet Institute

Appendix 2. The Council of Europe Convention on Cybercrime – National measures

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data,

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.