The future of netcrime now: Part 1 – threats and challenges

Sheridan Morris

Home Office Online Report 62/04

The future of netcrime now: Part 1 – threats and challenges

Sheridan Morris

Online Report 62/04

Foreword

This report describes the findings from research which asked a panel of experts to suggest responses to a number of criminal threats and technology challenges associated with the Internet and information technology applications in two to five years time. Their concerns were broad and diverse. New forms of old crimes (such as fraud) were identified, as well an increasing threat from new crimes (such as viruses and computer hacking). A common theme mentioned was that, as with previous product developments, information and communication technology can be misused in ways that were not foreseen by the providers. More particular to this study, the unpredictable convergence of technologies will continue to compound opportunities for criminal and malicious behaviour in unforeseen ways as it already has. The speed with which criminal opportunities develop is another significant factor and is reflected in the title of the report. Potential offences identified at the time of the research are already occurring as the report goes to publication.

The report concludes that there is no single solution to such threats, though a number of measures are proposed in the accompanying publication to this report, *The future of netcrime now: Part 2 – responses*. Rather the government, law enforcement and industry need to 'gear up' their capability to continuously look forward, attempting to identify new forms of criminal technology misuse as soon as they emerge, or even before they are seized upon by the criminal community. Only in this way will the numerous gatekeepers stay abreast of those who would abuse the opportunity the Internet and its related technologies has given us.

Dr Lawrence Singer
Series Editor
Research, Development and Statistics Directorate
Home Office
December 2004

Acknowledgements

I would like to thank all those who gave freely of their time as participating members of the Delphi panel. Those who were happy to be cited as panel members are listed in Appendix C. Dave Mann and Andrew Silke are also thanked for their time and contributions as members of the project co-ordination committee. Thanks also must be given to the Project Board members who contributed to the aims and the direction of the project; they were John Crow, Clive Harfield, David Ware, Vina Kapil and Tim Wright. Special thanks are also given to Paul Ekblom who provided valuable comments on earlier drafts of the report. I am especially indebted to Kathryn Hyde-Bales, who undertook the enormous task of administering all elements of the survey, including data collection and panel correspondence. It would not have been possible without her.

The author

Sheridan Morris is a Senior Research Officer in the Home Office Crime and Policing Group.

The Crime and Policing Group would like to thank Dr. Steven Furnell of the University of Plymouth for acting as independent assessor for this report.

Contents

Tables

Figures

Executive summary

This report describes the results of research seeking to identify emerging criminal and malicious behaviour threats relating to the misuse of computers and the Internet. It is a companion report to *The future of netcrime now: Part 2 – responses*. The research formed part of the Home Office Crime and Policing Group's Organised and Hi-Tech Crime Research programme.

Crime and abuse related to information and communication technology (ICT) is an increasingly topical subject, both in the media and in government. This research coincides with the publishing of e-crime and information assurance initiatives by the Home Office and the Central Sponsor for Information Assurance. The intention of undertaking this research was to play a part in the strategic development of UK information assurance, through its contribution to informing the Home Office e-crime strategy, and to inform policy makers and practitioners, pulling together diverse information assurance measures into a single, if summary, document. In looking to the future, other relevant programmes include the Department of Trade and Industry's (DTI's) Cyber Trust and Crime Prevention Project[1], which is part of the ongoing Foresight futures research programme.

Definitions

This paper has adopted the term netcrime (Mann and Sutton, 1998), defined here as 'criminal or otherwise malicious activity utilising or directed towards the Internet and/or information technology applications'. This definition extends beyond desktop or laptop computers, embracing all forms of networked device (e.g. hand-held computers of various forms and networked domestic appliances). It is also assumed that most criminal activity will involve such devices being connected to a Local or Wide Area Network, the Internet or a public telecommunications network. The terms computer, network and system will be used interchangeably throughout the report. The term *hi-tech* crime has been rejected as this could include technology developments outside the scope of networked information technology such as nanotechnology or bioengineering.

Method

The research involved the creation of a 'Delphi' panel of experts. There are various forms of Delphi panel, but the distinguishing characteristics are the use of structured questioning (e.g. questionnaires) to elicit the judgements of a panel of individuals, identified as experts in their field, on a given topic. As here, the exercise is conducted anonymously so as to encourage individuals to express their opinions, without reservation, alongside their peers. There was a broad range of government, law enforcement and regulatory representation on the panel, joined by experts from industry, academia and the voluntary sector, all of whom brought both a technical and non-technical expertise to the deliberations. Through the use of electronic questions, the panel, whose identities were unknown to each other, was asked nine broad questions, clustered around three themes. First they were asked to look at criminal threats, identifying what areas of Internet and information technology application they considered to be the possible focus of criminal activity in two to five year's time, the form such activities would take and the reasons for their response. Second, a similar set of questions was asked in relation to technology-based challenges and which have the potential to be misused by criminals and represent a challenge to law enforcement and/or legitimate users. Finally, the responses to these threats and challenges were explored from the perspective of UK law enforcement agencies, the UK government and the information and communication technology industries and IT users.[2]

Through two rounds of questionnaires panel members were able to put forward their views on the questions as well as commenting and rating the comments of the rest of the panel. Thus there was an element of peer review, as well as a ranking of the threats and challenges identified by the panel. The results from the forty-eight experts who contributed to the primary Round 1 questionnaire identified 101 criminal threats and 137 technology challenges for comment and ranking by the panel.

[1] http://www.foresight.gov.uk/

[2] The third set of questions concerning the responses will not be discussed here but in a related report, *The future of netcrime now: Part 2 – responses* (Morris, 2004).

Findings

Criminal threats

The criminal threats identified were diverse, varying from high profile, current concerns such as hacking and fraud to lesser known problems regarding espionage, money laundering and the emergence of grey and illegal online markets of restricted goods. For each of these categories, numerous forms of criminal threat were identified, involving different offences as well as numerous abuses of technology. The top three concerns were online paedophile activity (e.g. online grooming, pay-per-view websites of illegal images, sharing of images by offenders using peer-to-peer applications), fraud (e.g. theft of personal organisers containing sensitive personal information to execute fraudulent online transactions, identity theft against e-government services) and espionage (corporate, criminal and political spies, using techniques as diverse as social engineering and complex software).

Technology challenges

Technology challenges were as diverse as criminal threats. The highest rated single item related to the perceived ability of offenders to undertake secure (from law enforcement) communications via the use of email and associated technologies such as cryptography, steganography and anonymous remailers. The highest rated category of technology was the use of peer-to-peer or file sharing applications. Such applications vary from those commonly used for the illegal downloading of music and video (e.g. KaZaA), to more specialised applications built for security and anonymity, which can facilitate secure criminal communications. As well as facilitating criminal or malicious activity, some technologies were also a source of concern as they represented a security threat to legitimate users. Peer-to-peer applications were considered to represent a potential security breach to legitimate users, as were wireless networks, currently being deployed in both public and private environments. One of the broadest concerns reflected the use, or abuse, of the World Wide Web via individual websites. Websites themselves can represent a direct threat to users if they are designed to falsely capture sensitive personal information for fraudulent purposes. Indirectly, websites represent a threat as a number are a source of offending information, providing resources to offenders for a variety of offences, most cited being the provision of hacking tools and know-how. Finally, websites can be the targets of offending, falling victim to denial-of-service attacks or web defacements for example.

There are of course limitations to the findings. The Delphi method is based not on statistical extrapolation but rests on the informed judgement of its participants. The scope and complexity of the topics on which their views were sought is extreme and highly dynamic, and these findings are but a snapshot of opinions at the time of the survey.

Conclusions

This report describes new forms of old crimes such as fraud, as well as an increasing threat from new crimes such as viruses and computer hacking. A common element is that information and communication technology can be misused in ways that were not foreseen by the providers. Another theme is how the convergence of technologies has compounded the opportunities for criminal and malicious behaviour in unforeseeable ways, and will continue to do so. For example would the use of peer-to-peer based music piracy have become so prevalent if not accompanied by the roll-out of broadband connections to the home?

The report concludes that there is no single solution to such threats, though a number of measures are proposed in the accompanying publication to this report, *The future of netcrime now: Part 2 – responses*. Rather, the government, law enforcement and industry needs to ‘gear up’ their capability to continuously look forward, attempting to identify new forms of criminal technology misuse as soon as they emerge, or even before they are seized upon by the criminal community. Only this way will the gatekeepers stay abreast or ahead of those who would abuse the opportunities the Internet, and its related technology, has given us.

1. Introduction

The subject of information and communication technology-related crime and abuse is increasingly topical, both in the media and in government. This research coincides with the publishing of e-crime and information assurance initiatives by the Home Office and the Central Sponsor for Information Assurance. In looking to the future, other relevant initiatives include the Department of Trade and Industry's Cyber Trust and Crime Prevention Project, which is part of the ongoing Foresight futures research programme. All these initiatives begin to address, from their own perspective, elements of the concerns raised by this research. It is hoped that together all these initiatives may form the beginning of a coherent and comprehensive approach to ensuring a secure future for the UK's e-government and e-commerce success.

Introducing netcrime

Fifty-three per cent (13 million) of UK homes are connected to the Internet, along with 68 per cent of small and medium enterprises[3] (Ofcom, 2004). Offering unprecedented global access to information and individuals, the Internet represents a major societal force in areas as diverse as education, commerce, community formation or freedom of speech. Unfortunately it is equally amenable to misuse. Computer or hi-tech crime, or netcrime (the term adopted by this paper) is becoming an increasing concern to a variety of regulatory and law enforcement sectors. The information technology (IT) age in which we live means the scope for information technology-based crime and abuse is extensive and diverse. Those with a role to play in its reduction form an equally diverse community. Any consideration of netcrime will involve an examination of a broad range of technical and commercial sectors, numerous and overlapping government and law enforcement jurisdictions and an increasing number of non-governmental agencies and bodies. All of these must operate in a timely co-ordinated manner across their numerous individual sovereignties in a rapidly changing environment.

Definition

This paper has adopted the term netcrime (Mann and Sutton, 1998), defined here as 'criminal or otherwise malicious activity utilising or directed towards the Internet and/or information technology applications'. This definition extends beyond desktop or laptop computers, embracing all forms of networked device (e.g. hand-held computers of various forms and networked domestic appliances). It is also assumed that most criminal activity will involve such devices being connected to a Local or Wide Area Network and/or the Internet. The terms computer, network and system will be used interchangeably throughout the report. The word 'application' has been used to suggest that the concern is not just with developments in hardware and software, but changes in the societal applications of current and future technology. Such changes may be driven by political, economic or cultural reasons. The term *hi-tech* crime has been rejected as this could include technology developments outside the scope of networked information technology such as nanotechnology or bioengineering.

Before discussing various forms of netcrime (fraud, extortion, espionage, paedophilia) the role of computers clearly varies and it is around this role that most high level definitions revolve. The author puts forward the following three categories – a computer network[4] can be the *target* of criminal activity or it can function as an intermediary for crime, either as a *medium* or *facilitator*. The phrase *criminal activity* is taken to include not only the activity of criminals (those operating for personal financial gain) but also others with different motivations such as threats to national security or the national interest from politically-motivated groups (Information Management & Computer Security, 2001:1, 2001: 2).

Computer as target of crime

Hardware theft

The most obvious form of a computer as the target of crime is the physical theft of computers themselves. Although this does occur (e.g. theft of individual laptops), the bulk theft of computer components, such as memory or processor chips also occurs. Such theft is undertaken either by hijacking the components in

[3] Businesses that employ up to 250 employees and have a minimum annual turnover of £50,000.

[4] No explicit distinction will be made between 'computers' (e.g. desktop or centralised systems) and the network which connects them, as networks are themselves made up of computers (e.g. routers) and all 'computers' require network connectivity to operate, so they should be seen as an integrated system (albeit one which may be separated into elements such as network for certain administrative or operating reasons).

transit or the removal of the chips from operating computers during the burglary of commercial premises. Looking forward, significant hardware theft may return as new powerful personal organiser or personal digital assistant (PDA) devices such as the Palm Pilot become more popular and valuable. Their size will make them as easy to steal as mobile phones (this concern is discussed in Chapter 2).

Data: confidentiality, integrity and availability

Other than the physical protection of computers from theft, most information technology security has traditionally been concerned with three key principles; maintaining the *confidentiality*, *integrity* and *availability* of system data.

Confidentiality is the simple concept that data must not be disclosed to those who are not authorised to receive it (e.g. its theft, interception or more commonly, copying). The unauthorised disclosure of information may be motivated by many things other than criminal personal gain including personal malice, economic or political espionage and a variety of political motivations. The theft, copying or interception of data may be an offender's prime, convertible or transitional target (Newman and Clarke, 2003). The copying of trade secrets may be considered the prime or final target for an offender motivated by commercial espionage. In contrast, network intruders (e.g. hackers) may seek network or user information as part of an ongoing process to gain greater access to a system and ultimately a database. Whilst such hacking is an offence in its own right, it is but a transitional target to database access and credit card details it may contain. Finally, the copied credit card details may be later used in the committal of online frauds and thus categorised as convertible targets (e.g. the credit card information is converted to a means of purchasing online goods and services). Although most information security may focus on online systems (e.g. preventing hacking), information confidentiality can be breached physically. Often overlooked is the low-tech physical copying and removing of information, installed on a CD or a key ring-sized storage device. Malicious but inadvertent unauthorised disclosure can also occur if a virus or worm infects a system and then randomly emails stored documents to addresses held in a contacts list.

Data integrity is an issue if there is evidence or even suspicion that unauthorised system access and data modification has occurred through changes in file details such as size or when last accessed (a new file access date may also indicate a data confidentiality breach). If, for example, the accuracy of stored information in a banking system was questioned the implications would be immense; if they were incorrect in a medical system they could be fatal (Information Management and Computer Security, 1995). The threat of such corruption can form the basis of extortion threats against organisations. Viruses and other malicious software can also cause data to be destroyed or partially corrupted.

Data availability is a product of computer or network availability, a concept best illustrated by the inconvenience experienced by users when an office system or Internet website becomes unavailable or 'goes down'. Malicious attacks against websites are generally referred to as a 'denial of service' attack. A denial of service (DoS) attack can be defined as 'actions that prevent any part of a system from functioning in accordance with its intended purpose' (Power, 2000:330). Most attacks are in fact 'distributed denial of service' (DDoS) incidents, the impact of the attack being magnified by hitting the target from multiple computers.

The availability of systems are attacked in numerous ways including hacking, malicious software and denial of service attacks. What is often overlooked, however, is low-tech, physical attacks on computer facilities or network cabling. Whilst most major computer facilities such as webhosting centres have high physical security, private power supplies and sophisticated fire controls, network cabling between sites is more vulnerable.[5] Such incidents are of particular relevance to those concerned with the integrity of the telecommunication elements of the critical national infrastructure. The critical national infrastructure can be defined as 'those parts of the United Kingdom's infrastructure for which continuity is so important to national life that loss, significant interruption, or degradation of service would have life-threatening serious economic or other grave social consequences for the community, or any substantial portion of the community, or would otherwise be of immediate concern to the government.' (NISCC, 2003).

Computer as intermediary of crime

As computers have become increasingly widespread in modern society so their use in criminal activity has increased, reflecting a recurring pattern in the use and misuse of technology. As an intermediary, computer systems are viewed as acting as a buffer between offenders and their victims, affecting how an offence is undertaken or executed (*medium*) – the criminal *modus operandi*. Similarly computers can enable

[5] An example of such attacks can be found at http://news.zdnet.co.uk/story/0,,t269-s2124353,00.html

communications between offenders in a global, near real-time and relatively secure manner (*facilitator*). The Internet can also facilitate offending through its ability to provide intelligence, and in many contexts direct tools for offending (e.g. hacking tools). Computer as an offending medium considers the offender-victim/conspirator contact, whereas computer as offending facilitator considers the offender-offender contact. The difference between these categories is often a matter of emphasis. It is possible for computers to play both roles in a single offence such as an Internet e-commerce-based fraud (medium) which may also involve significant online communication between offenders (facilitator).

Computer as medium

Much crime encountered through the Internet may be considered as 'old crimes, new medium'. An example of this is 419 fraud. This fraud involves the victim receiving an unsolicited request from an overseas individual requesting assistance in transferring large amounts of money out of his/her country due to unfortunate circumstances. In return for the victim's assistance by providing bank details to receive the money, he/she will receive a percentage of the transfer. At the last minute the victim is asked to forward a cash advance to pay 'banking fees' which will be repaid along with his/her commission for helping the funds transfer. After the cash is advanced the transfer does not take place and the overseas individual disappears. This established scam has kept its essential confidence trick element whilst moving from unsolicited postal mail, then faxes and now email as the offenders seek to con the gullible and the greedy. However the offender contacts the victim the objective is fraud, something recognised in UK legislation which does not explicitly take into account how the offence is committed. Similarly, the Internet can act as merely another distribution channel for offenders (e.g. the online selling of obscene material). In contrast to 'old crimes, new medium' is what may be considered 'new crimes for a new medium' (e.g. the Internet). Examples would be computer as target category offences such as hacking, virus writing and denial of service attacks.

Computer as facilitator

Organised offenders, be they criminals or terrorists, often require a command, control, communication and intelligence gathering capability to operate effectively, particularly if they are insulated from each other by geography, anonymity or surveillance threats (i.e. offenders may be in close proximity to each other but wary of contacting each other due to concerns that they are under surveillance). The dramatic growth of the Internet and its underlying technology, along with a more recent growth in mobile telephony and now wireless communications, has reduced the efficacy of traditional telephone surveillance techniques. Previously, communications surveillance had to contend with monitoring perhaps a small number of fixed lines at static addresses and registered mobile phones. Computer and communication services are now widespread, with the miniaturisation and increasing sophistication of affordable devices. Conversations, along with email and data files can now be sent and received on the move from unregistered mobile phones and other portable computing communication devices using non-registered Internet access (discussed in Chapter 2 under the technology challenges of portable computing and communication devices).[6] Powerful and secure communications can be utilised via personal computers using Internet-based services such as newsgroups, mail lists, chat rooms, peer-to-peer services (discussed in Chapter 2) and, of course, websites.

Other definitions include the early work by Carter (1995, cited in Casey, 2000) who proposed the following computer crime categories:

- computer as target (e.g. computer intrusion, data theft, techno-vandalism, techno-trespass);
- computer as the instrumentality of the crime (e.g. credit card fraud, telecommunications fraud, theft or fraud);
- computer as incidental to other crimes (e.g. drug trafficking, money laundering, child pornography);
- crime associated with the prevalence of computers (e.g. copyright violation, software piracy, component theft).

The first three categories resemble those proposed by the author, whilst it could be said that all incidents covered in the fourth category can be accommodated by one of the previous three (e.g. contemporary copyright violation in the form of downloading music files is copyright crime using the medium of the computer and the Internet). Casey (2000) makes the point, however, that such categories omit the role of computers as a source of evidence for investigations, whatever the crime or the role of the computer.

[6] Such devices include both wireless-enabled personal digital assistants such as a Palm Pilot, as well as mobile phone-based devices which now include keyboards such as the Blackberry.

Whilst it might be assumed that computers may be such a source of evidence whatever their role, this is perhaps a function worth noting.

Whatever the device or medium, offenders can now communicate with each other irrespective of physical location using numerous and ever evolving channels. The 'death of distance' was the first barrier to go for internationally mobile offenders with the development of the Internet and basic services such as email. For instance, dispersed and anonymous paedophiles found each other, forming self-supporting communities, strengthening and feeding their desires via bulletin boards, websites and newsgroups. Such activity is now facilitated by the next generation of communication platforms, chat rooms and peer-to-peer tools. Similarly international organised criminals and terrorists may now communicate using old techniques in a new medium such as cryptographic and steganographic[7] communications or covert messages in public spaces (e.g. chat rooms, personal ads, auction sites etc).

Aims and objectives

This research formed part of the Crime and Policing Group's Organised and Hi-Tech Crime Research programme. The aim of the research was to identify emerging criminal and malicious behaviour threats relating to the misuse of computers and the Internet, along with insight into corresponding responses and countermeasures. Such threats include ever evolving old offences committed in the new online medium and new offences that may brought about by technological or societal change. The study had three key objectives.

(i) To identify what areas of Internet and information technology application will be the possible focus of criminal activity in three to five years time?

(ii) To examine what areas of Internet and information technology possess the potential to be misused by criminals and represent a challenge to law enforcement?

(iii) To explore how various sectors can prepare for such threats and challenges.

This report examines the results of objectives one and two, with a separate report examining the results of the third objective (*The future of netcrime now: Part 2 – responses*, Morris, 2004). In attempting to generate insight to the future, one of four different methodologies tend to be employed: forms of consensus; extrapolating on trends; historical analysis and analogy; and the systematic generation of alternative future paths such as scenario analysis (Lang, 1995). The offences and behaviours this study sought to consider are highly diverse but are linked by a common absence of recorded offence data. This is because most legislation is technology or *modus operan*di neutral and makes no specific reference to the role of computers or the Internet in its committal (the Computer Misuse Act 1990 being the main exception in covering unauthorised system access such as hacking and virus writing). There is little or no official offence data (other than that generated by commercial surveys and data sets) with which to undertake quantitative trend analysis (Hyde-Bales, Morris, Charlton, 2004). Also, as this study sought to identify the new and unexpected, it was clear that the output would be qualitative in nature and hence the Delphi methodology was selected for the purposes of this study.

In undertaking such a forward-looking exercise it was hoped the findings would contribute to strategic threat assessments and broader futures work undertaken by other governmental and law enforcement organisations (e.g. National Hi-Tech Crime Unit), as well as pulling together numerous and diverse concerns into a single, if summary, briefing document for new policy makers or practitioners with an interest in this area. This research has already contributed to the formulation of the Home Office e-crime strategy and ongoing work in this area.

[7] Steganography concerns the 'hiding of information'. Cryptographic information is in plain view but encrypted to remain secure. Steganographic information, in contrast, is concealed or embedded in another object, which itself may remain in plain view. A modern digital example would be the hiding of secret bank account details in an apparently innocuous photograph that is posted in plain view on the Internet or distributed by email.

Methodology

The Delphi method

The Delphi method is a form of 'futures research' that seeks to inform perceptions, alternatives and choices about the future. The technique was developed during the early 1950s by the RAND Corporation for military applications and has developed into three key formats (Woudenberg, 1991).

- The Conventional Delphi, as loosely used here, has two common applications, forecasting and estimating unknown parameters. The technique is often, except here, used to facilitate consensus on an issue amongst a number of individuals or groups.

- The Policy Delphi does not aim for consensus but seeks to generate the strongest possible opposing views on the resolution of an issue and to table as many opinions as possible.

- The Decision Delphi is used to reach decisions amongst a diverse group of people with different investments in the solution. (Lang, 1995).

Furthermore, a Delphi approach may also be combined with other futures techniques such as the use of scenarios. The Delphi technique may be found in areas where there is an absence of sufficient data and/or an incomplete theory on cause and effect in regard to the area under study. Sitting between knowledge and speculation, the outcome of the panel may be considered informed judgement. Given the diverse, interrelated and fragmented knowledge sets under examination it was deemed a suitable method for examining this area and indeed follows in the footsteps of similar research (Coutorie, 1995; Tafoya, 1986).

A conventional Delphi study (hereafter referred to simply as the Delphi) was adopted for this research and involved the convening of a panel of a relevant 'experts' regarding netcrime and associated issues. Such a Delphi has four basic features (Lang, 1995; Woudenberg, 1991).

- *Structured questioning* achieved through the use of questionnaires. This aims to keep participants' responses focused and enables the channelling of many inputs into a compact output.

- *Controlled feedback* achieved by feeding back to the panel members the responses of the group, as well as their own response, for their reconsideration. This means that all the responses of the panel are taken into account.

- *Iterations* is the process by which the questionnaire is presented over at least two rounds to enable participants to reconsider their responses.

- *Anonymity of response* is achieved through the questionnaires, ideally giving group members the freedom to express their opinions without feeling pressured by the wider group.

The Delphi panel is an attempt to 'generate the positive interaction of views of a group but avoid the negative group dynamics that may emerge, such as domination by key individuals, falling into a rut of pursuing a single train of thought, pressures to conform and becoming burdened with periphery information' (Preble, 1983). It is acknowledged that such a written interactive process may lack some of the potential 'brainstorming' stimulation that can emerge in the best group situation, but it was felt the benefits and the opportunity for considered answers outweighed these potential negative factors.

The expert panel

The composition of the expert panel is the cornerstone of the Delphi method as rigorous method and analysis cannot compensate for weak input. As the scope of the criminal and technological threats that may emerge are broad, it was essential to gather a broad church of knowledge and opinion from differing sectors. For every criminal threat it is likely that there may be both a law enforcement and technological perspective (e.g. breaking into a computer network presents technical prevention and investigative detection issues). Such a dual approach is further complicated by the organisational and technical complexity of much Internet activity where examining one particular concern might involve numerous parties. Finally, in examining any single issue different perspectives were sought. Thus security concerns regarding a singular technology might be addressed by those who built it (a vendor); those who deploy it

(information technology security); those who use it (government or consultants); and those who may study it for weaknesses (academics). The dominant theme of this study was concern over criminal and malicious behaviour, hence there was a broad range of government, law enforcement and regulatory representation. Technical complexity was a significant but not sole focus of this study and the panel composition. Furthermore, some topics were given explicit recognition by the inclusion of participants with specific knowledge and experience in online paedophilia, fraud and piracy. In attempting to seek out as diverse an opinion as possible, consideration was given to seeking the participation of members of the hacker and warez community regarding hacking and piracy respectively. This approach, as adopted by Coutorie (1995), was abandoned as it was considered too problematic to validate the experience and competence of such participants, along with concerns over the confidentiality of the study.

Potential panel members were identified from numerous sources including published literature, conference presentations or were otherwise known from their participation in certain forums. In some cases relevant organisations (e.g. significant information and communication technology businesses) were approached and they in turn proposed a representative. Similarly specialist law enforcement, government and not-for-profit organisations were approached and a suitable representative requested. The need for informed rather than senior representation was emphasised.

Table 1.1 summarises the sectors from which participants were drawn. Academic researchers were largely from computing and engineering disciplines but did include those from a criminal justice perspective. Government representatives covered a variety of broad issues from a regulatory and policy-making perspective. Law enforcement included individuals from diverse police- and security-oriented agencies, representing experience in a broad range of criminal offences. Fraud takes many forms on the Internet and was addressed by a number of practitioners from legal and financial perspectives.

Information technology security is a very broad field and this was reflected in the differing perspectives participants brought. Some respondents could be considered 'users' in that they managed security for commercial organisations, whilst others represented service providers such as telecommunications, Internet Service Providers (ISPs) and webhosting companies. Others involved in broader information technology risk management consultancy also made up this group. A number of individuals specifically involved in tackling piracy (software and entertainment content) and online paedophilia in different capacities boosted input on these areas.

Table 1.1: Panel sector composition

Sector	Nos. of respondents	Percentage
Information technology security	17	35
Law enforcement	8	17
Academic research	7	14
Fraud	6	12
Government	3	6
Piracy	3	6
Online paedophilia	3	6
Information communication technology vendor	2	4
Total	**49**	**100%**

Seventy-three individuals were invited to participate in the study, of which 53 agreed to do so. Forty-eight actually participated in the first survey round, of whom 46 provided academic and experience details. More than half of these were graduates (56%), almost a third (29%) postgraduates (e.g. masters degrees or postgraduate certificate) and a quarter (27%) either held doctorates or were undertaking doctoral studies. Half of the panel (51%) possessed industrial or professional qualifications and certifications.

As well as their formal qualifications, respondents were asked to indicate on what topics they felt confident to comment based on the number of years experience they had in an area. Table 1.2 details the number of respondents and the accumulative years of experience represented by the panel in a number of particular topics. For individuals with broad roles their experience may contribute consecutively to many categories. That is, an experienced systems security specialist, for example, may have 20 years experience in each of the following: system security, computer crime investigation and digital forensics (having been the victim of hack attacks) and malicious software (patching and repairing the system after major virus outbreaks). Respondents may also have experience in the same category but from differing perspectives. A forensic

accountant and a police officer may be brought in to investigate a company fraud; the system administrator may be required to search for evidence on the computer; and a specialist lawyer may prosecute (or defend) the case.

Table 1.2: Panel experience composition

Topic experience	Nos. of respondents	Cumulative experience (years)
Fraud	25	271
System security management	27	267
Computer crime investigation	30	201
Information assurance	19	188
Malicious software	21	180
Encryption	20	165
Online privacy, anonymity issues	20	163
Counter-espionage	12	119
Digital forensics	15	118
Digital piracy and counterfeiting	14	81
Online activism and protest	8	47
Online harassment	7	39
Social service issues (e.g. child protection)	8	36

The survey

The research employed four questionnaires over two rounds. Questionnaires took the form of electronic spreadsheets, distributed largely by email. Written guidance accompanied each questionnaire and respondents were able to email or telephone with any queries (though very few were received).

Round 1: Questionnaire 1

An initial short netcrime questionnaire was circulated to panel members. These questions were intentionally loose and open-ended to allow participants free reign in their responses. Questionnaire 1 contained five primary and four supplementary questions, allocated into two sections. Section 1 contained two primary questions (questions 1 and 4), each with two identical supplementary questions and considered future criminal threats and challenges to law enforcement.

Question 1 asked respondents to identify a high level threat (e.g. online fraud), whilst question 2 asked them to illustrate what form the threat may take (e.g. online transaction websites being defrauded by the use of stolen credit cards for online goods or services). A question 1 response was often accompanied by two or more question 2 responses. Question 3 asked respondents to provide some indication of the rationale for their responses to questions 1 and 2, so that other respondents might better understand and consider their responses. The validity of the panel responses was not assessed for accuracy by the co-ordination committee as it was felt that any such inaccuracies would be picked up the panel peer review phase in Round 2. Questions 4, 5 and 6 regarding technology challenges took a similar format.

> Question 4: What areas of Internet and information technology do you consider possess the potential to be misused by criminals and represent a challenge to law enforcement and/or legitimate users?
>
> Question 5: What form do you think these activities will take?
>
> Question 6: What are your reasons for this expectation?

Whilst question 1 was interested in behaviour that was explicitly criminal or malicious, questions 4, 5 and 6 were concerned with technology that possessed a potential for criminal or malicious use. Whilst network monitoring tools are developed for legitimate purposes, a number can be used for malicious purposes (e.g. hacking).

Questions 7, 8 and 9 were concerned with respondents' opinions on what needs to be done to prevent or mitigate the threats and challenges outlined in questions 1 to 6.

Question 7: How should UK law enforcement agencies prepare for such threats?

Question 8: How should the UK government prepare for such threats?

Question 9: Globally, how should the information and communication technology industries and IT users prepare for such threats and challenges?

As with questions 1 to 6, panel responses were not assessed in terms of accuracy or suitability by the co-ordinating committee. In a number of instances where suggestions were made for initiatives that already existed, other panellists recognised such inaccuracies and these have been cited in the relevant discussion.

Round 2

There was substantial response overlap as respondents identified many commonly perceived criminal threats and technology challenges. Examples included threats from fraud and online paedophilia and technology challenges presented by mobile computing and communications devices. Where such duplication existed responses were aggregated into a reworded single response (e.g. ten entries for more police training were combined into a single entry on this point). Once responses to all nine questions had been aggregated they were fed back to the panel over three second round questionnaires covering criminal threats, technology challenges and preventive responses. Each questionnaire contained the items (threats, challenges or responses) identified in Round 1, clustered around key themes. Respondents were presented with a number of forms the item might take, along with some explanation for its inclusion by members of the panel. They were then invited to comment on each item and rate it. This second phase comment and rating process served as the group feedback function, as each panel member was able to anonymously feedback on the comments of all others. Figure 1.1 provides examples of these second round questionnaire items.

Figure 1.1: Examples of Round 2 questionnaire items

Questionnaire 2: criminal threats			
Q1.Criminal threat	Q2. Form it might take	Q3. Reason for expectation	Q3. Reason for expectation
Commercial espionage (employee)	Unauthorised disclosure of information, by various means, by employees' for personal gain or emotional reasons.	Job turnover eliminates company loyalty in place of ambition /disaffection.	Belief that crime cannot be detected.

Figure 1.2: Examples of Round 3 questionnaire Items

Questionnaire 3: technology challenges			
Q3.Technology challenge	Q4. Form it might take	Q5. Reason for expectation	Q5. Reason for expectation
Anonymity (lack of access authentication)	Ability to 'safely' send illegal communications (content or intent) due to lack of authentication required for Internet café or kiosk service.	Criminals will exploit pay-as-you-go mobile Internet connections, & applications that conceal or delete routing details.	Commercial and political pressures to provide Internet access with few/no checks.

Figure 1.3: Examples of Round 4 questionnaire Items

Questionnaire 4: responses	
Q8. UK government response	
Awareness promotion	Continual efforts to raise awareness amongst users and gatekeepers (e.g. parents, teachers, librarians) about safety and new technologies. Companies need to look to their own individual strategies but also fund charitable and joint efforts.

The panel members were recruited during September 2002 and the survey conducted between October 2002 and February 2003. If crime prevention knowledge is a depreciating asset, then any futures oriented warning and information this paper seeks to provide will depreciate faster than most such publications due to the rapid development and application of the technology discussed. Even whilst conducting this survey, a number of items that appeared new and original in the first data collection round, were subsequently reported in technical journals and some offences even made their way to court.

The co-ordinating committee

Co-ordinating committees, or monitoring teams, are often found in the administration of Delphi projects. Administering Delphi research often involves subjective decisions when processing respondent contributions. In this research this subject processing focused around aggregating the respondent results as previously discussed. To avoid or minimise individual biases, the primary researcher was joined by two other researchers to form a project co-ordinating committee. Whilst these individuals were from the same organisation as the primary researcher, they were both experienced researchers with differing academic backgrounds. Furthermore, a taxonomy was used to provide a structured means of aggregating respondent contributions, where differences in language and phrasing could obscure similarities and subtle differences in proposed threats and challenges.

Structure of the report

The remainder of this report is broken down into two chapters. Chapter 2 outlines the survey results in detail, followed by two sections discussing the criminal threats and technology challenges identified by respondents. Chapter 3 will summarises and provides concluding remarks on what the threats and challenges discussed mean to the UK and ways forward.

The companion report to this publication, *The future of netcrime now: Part 2 – responses* (Morris, 2004), discusses the results of questions 7, 8 and 9: the panels views on what government, law enforcement and industry and users need to do to meet the issues raised here.

2. Findings

Round 1: Questionnaire 1

Of the 53 questionnaires issued in Round 1, forty-eight (91%) were returned. A total of approximately 2,500 comments were submitted by the panel. These were aggregated down to 425 items, allocated across the three questionnaire categories: criminal threats (101), technology challenges (137) and netcrime responses (187).

Round 2

Round 2: Questionnaire 2 (criminal threats)

One hundred and one criminal threats were put forward for comment and rating in Questionnaire 2. The threats were clustered around thirteen high level categories that emerged from a review of the responses:

- critical national infrastructure/infowar;
- denial of service attacks;
- espionage;
- extortion;
- fraud;
- hacktivism;
- non-categorised.
- hardware theft;
- malicious software;
- market abuse;
- money laundering;
- online paedophilia;
- piracy; and

A non-categorised section was used for all other items that did not fit into the 12 other categories. This included items relating to topics such as spamming (the sending of unsolicited emails) and online gambling. Thirty eight out of the 48 (80%) Round 1 participants completed the second questionnaire and rating, providing 947 additional comments on the 101 identified threats.

Round 2: Questionnaire 3 (technology challenges)

One hundred and thirty-seven technology challenges were put forward for comment and rating in Questionnaire 3. The threats were clustered around nine high level categories that emerged from a review of the responses:

- anonymisation;
- broadband;
- email;
- encryption;
- mobile communications;
- peer-to-peer;
- wireless;
- webhosting; and
- non-categorised;

Twenty-nine out of the 48 (61%) Round 1 participants completed the third questionnaire and rating, providing 1,152 additional comments on the 137 identified technology challenges.

Round 2: Questionnaire 4 (netcrime responses)

One hundred and eighty seven responses to netcrime were put forward for rating in Questionnaire 4. Responses were clustered around eight categories, that again emerged with the panel results:

- strategy and research;
- legislation, prosecution and standards;
- awareness and alerts;
- prevention and security;
- reporting and recording;
- communication and cooperation;
- policing;
- resources, tools and training.

Twenty-eight out of the 48 (58%) Round 1 participants completed the fourth questionnaire and rating, providing 1,493 additional comments on the 187 proposed netcrime responses.

The remainder of this report will now discuss a number of the identified criminal threats and technology challenges in more detail. Data from Questionnaire 4, responses to netcrime, is published separately in the publication *The future of netcrime now: Part 2 – responses.*

Table 2.1 details the allocation of the 101 criminal threat responses and 137 technology challenges across the high level 13 categories. Both criminal threats and technology challenges feature a non-categorised category for items that did not fit the preceding clusters.

Table 2:1: Criminal threats and technology challenges

Criminal threat category	Number of threats	Technology challenges category	Number of challenges
Fraud	20	Mobile communications	13
Espionage	10	Webhosting	11
Paedophilia	12	Email	9
Market abuse	2	Peer-to-peer platforms	9
Piracy	8	Wireless	8
Malicious software	8	Broadband	7
Extortion	8	Cryptography	5
Denial of service attacks	5	Anonymisation	4
Money laundering	4	Non-categorised	71
Hacktivism	4	-	-
Critical national infrastructure/infowar	5	-	-
Hardware theft	3	-	-
Non-categorised	12	-	-
Total	**101**		**137**

Threat and challenge ratings

Respondents rated the threat level of each criminal or technology item in three to five years, compared to the current time. Each item was rated across as highly significant (1), significant (2), no change (3), less significant (4) or insignificant threat (5). These terms were not defined; their primary purpose to allow items ranking. Other options available to respondents were 'Unwilling to Comment' and 'No Knowledge'. As the panel had a broad and diverse knowledge base it was to be expected that there would be areas that individuals were not competent to comment on. The two categories 'unwilling to comment' and 'no knowledge' enabled the survey to differentiate between respondents who were knowledgeable in an area but were unwilling to make an educated threat rating on an item, from those who were simply inexperienced or unaware of a certain topic. Average rating scores were calculated for each threat or challenge item, based on the number of respondents who rated the item. The number of respondents who rated each item (excluding those who indicated they were either unable or unwilling to rate the item) is indicated alongside each item in the following tables and Appendices A and B.

The data produced in this study were inherently qualitative. The purpose of the rating exercise was merely to serve as a notional indicator of potential priority areas for research, policy and law enforcement stakeholders when faced with over 200 threats and challenges. The range of responses for criminal threats was rated 1.88 to 3.06, with an average of 2.34. The range of responses for technology challenges was rated 1.57 to 3.22, with an average of 1.65. Just over half (55%) of all criminal threat ratings graded items as either 'highly significant' or 'significant' threat in three to five years time. In contrast only five per cent of criminal threat ratings graded items as either 'less significant' or 'insignificant threat' in three to five years time. The remaining 40 per cent indicated no change on an item. A similar picture exists for technology challenges. More than half (64%) of all criminal threat ratings graded items as either 'highly significant' (1) or a 'significant' threat (2) in three to five years time. In contrast only seven per cent criminal threat ratings graded items as either 'less significant' or 'insignificant threat' in three to five years time. The remaining 29 per cent indicated 'no change' on an item. As respondents were uniformly disposed to positively rate threats or challenges items, no items emerged as particularly highly rated.

Space limitations require that only a selection of items be highlighted and briefly discussed in the body of this report (see Appendices A and B for the full list of criminal threats and technology challenges along with their panel ratings). In deciding which items to discuss, a number of items were excluded on the grounds they were currently recognised, documented and the subject of substantial action by various parties. For instance, a number of threats regarding online paedophilia were highly rated by the panel, but are not explicitly discussed in this report as they are documented and addressed by various government departments (e.g. Home Office Internet Task Force on Child Protection) and law enforcement initiatives, as well as dedicated publications (Carr, 2004; McVean and Spindler, 2003). Examples include the risks of online grooming of victims in chat rooms or on mobile phones and the distribution of illegal images by organised crime groups or peer-to-peer technology. Other excluded items include a number that are highly technical, the subject of specialist discussions and considered outside the audience of this report. An example of such items would be possible manipulation of computers running the Border Gateway Protocol.

The following discussion has attempted to focus on issues that represent either an *emerging threat* or may be examples of *transitional targets* (or technologies) that represent a channel or means to numerous forms of criminality or abuse. In considering newly emerging issues it should be stated that many items have already been discussed in specialist forums and a number are already starting to be committed; a number of such forums or organisations will be cited alongside a relevant threat or challenge. In responding to fraud for example, many threats identified by respondents have been discussed to varying degrees by forums such as the UK Fraud Advisory Panel or the USA Internet Fraud Complaint Centre. Other bodies are trade- (i.e. manufacturers) or standards-related. The GSM Association globally represents more than 585 GSM mobile phone service operators and played a key role in the UK initiative to tackle mobile phone theft and cloning. Similarly the Wi-Fi Alliance, a non-profit international association of 205 member organisations, is seeking to promote greater security in the roll-out of wireless networks with technical standardisation and guidance. On a more informal basis, Internet newsgroups and bulletin boards play a prominent role in discussing issues, particularly technical ones, such as hacking, network security and encryption. However, many such discussions have hitherto been outside the knowledge of more mainstream practitioners and stakeholders and are thus considered worthy of flagging here.

It also has to be acknowledged that all items discussed are those as identified by the panel respondents. In examining the highlighted criminal threats and technology challenges this report seeks only to provide a brief introduction to the issue. Where further information is available it will be identified.

3. Criminal threats

There were a number of panel responses, that whilst entered in answer to the criminal threat question, served to highlight a technology misuse issue. Equally, in highlighting a technology challenge respondents outlined an offence not covered elsewhere. There is then overlap, as there is between the 13 high level categories that have been adopted in this following discussion. For instance, malicious misinformation regarding an individual can also serve as a form of extortion. Online gambling can serve as a means of money laundering or fraud depending on how it is manipulated.

Money laundering

A broad definition of money laundering is that it is the process whereby criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it allows them to maintain control over these proceeds and, ultimately, to provide a legitimate cover for their source of income and the financing of their criminal activities.[8] All of the threats detailed here have been recognised and documented by the Financial Action Task Force (FATF) on Money Laundering (FATF 1998; 2000; 2003). Table 3.1 details five ways in which the Internet could facilitate money laundering, as identified by the panel.

Table 3.1: Money laundering threats

	Rating	N=
Overseas online banking: money laundering via increased access to overseas 'virtual countries', allowing the bypassing of financial monitoring & other policing measures.	2.06	16
Overseas online gambling: money laundering via increased access to overseas electronic gambling, allowing the bypassing of financial monitoring & other policing measures.	2.18	17
Electronic cash: potentially non-existent paper trail.	2.19	16
Online share purchasing: money laundering via increased access to online share trading, allowing the bypassing of financial monitoring & other policing measures.	2.33	15
Online escrow services: money laundering via increased access to fraudulent Internet escrow services, allowing the bypassing of financial monitoring & other policing measures.	2.44	16

Despite the activity of the FATF, respondents highlighted the absence of adequate legislation in non-FATF members countries, along with how the absence of physical face-to-face contact reduced the ability (or requirement) of organisations to identify and authenticate individuals when opening online financial accounts for an increasing number of online banking services (the 'know your customer' challenge). Once accounts were opened they could then be accessed from anywhere in the world, twenty-four hours a day and again without authentication of who was physically operating the account. Both these factors facilitate the *placing* and *layering* stages of money laundering. Placing is the first stage of money laundering and requires the insertion of illegally acquired cash into the legitimate economy in a manner which distances it from its source as much as possible (e.g. opening of a bank account(s) with funds). Subsequent layering is the first stage of attempting to conceal the source and ownership of the money by disrupting potential audit trails (e.g. moving money between numerous accounts, often internationally). The potential role of 'virtual purses' as a form of electronic cash was raised. The virtual purse form may be transformed with its incorporation into mobile phones and portable computing devices to enable virtual payments to various machines. In the Asia-Pacific region vending and ticketing machines now accept payments from such phones, whilst the phones themselves can be 'topped up' from the next generation of cash machines (ARC Group, 2002).

In money laundering parlance, virtual purses or other forms of e-cash may be considered as the latest forms of 'informal money or value transfer systems' (IMVT) (FATF, 2003:6) as they can take place outside the conventional banking system through non-bank financial institutions or other business entities (though they may interconnect with the formal banking system in places). Online gambling via Internet casinos was specifically targeted in the latest FATF recommendations (FATF, 2003).

[8] The UK definition is far broader. As defined by the Proceeds of Crime Act 2002 (one of many acts to tackle money laundering) money laundering can involve the possession or simple spending of the proceeds of crime (e.g. even money from a mugging).

Fraud and theft

Many forms of online fraud are offences of obtaining services dishonestly, where a person seeks to avoid payment. Deception is not an essential part of the offence and therefore extends to obtaining services or goods by providing false information to computers. A number of forms of fraud and theft identified in this study have not been highlighted here because they are well established and various counter-measures are emerging. Examples include auction fraud, the non-delivery of goods and 419 fraud. Payment card fraud is not new but new forms of obtaining card details continue to emerge. For the UK the Association for Payment Clearing Services[9] reported fraud losses of £45 million for Internet based transactions, up 68 per cent on the £28 million identified in 2002. An Experian 2001 survey identified that 52 per cent of UK online retailers indicated Internet fraud was a problem, 55 per cent believing it was increasing. Most fraud is against online merchants but as the vision of e-government gains substance then such transactions may be targeted. Offenders target not only e-commerce businesses and consumers, but also use the Internet as another means of reaching ordinary consumers with ever evolving false professional or leisure services (e.g. numerous forms of gambling). Table 3.2 details the 12 ways, identified by the panel, in which the Internet facilitates fraud in its various forms.

Table 3.2: Fraud threats

	Score	N=
Payment card abuse		
E-commerce (stolen card details by hacking or intercept): unauthorised copying of credit card information, obtained via various means (system penetration, data tap using wireless networks, or a pass-through site), to achieve online authentication & purchase of goods/services.	2.33	30
E-commerce (credit card information capture by 'page jacking'): legitimate website corruption by modifying pages or DNS re-direction, fooling users to enter credit card details to a fake webpage; captured credit card details then used for purchases etc.	2.44	25
E-commerce (key logger): unauthorised copying of personal information and credit card details by a covertly installed key logger application at third party terminals (e.g. cybercafe, library, college), to achieve online authentication & purchase of goods/services	2.62	26
Identify theft		
Identification systems (e.g. smart cards): illegally produced and false documentation used to further illegal activity e.g. fraud.	1.71	14
E-Govt. (identity theft): fraud against online government services (VAT, Income Tax, Tax Credits, DTI licensing) via various techniques (hijacking corporate or individual identities).	2.05	22
General Fraud (false document production): online data mining (chat rooms, newsgroup, databases, questionable credit reference agencies) to produce false documentation (passport, 'smart' ID cards, medical records) to achieve offline authentication.	2.08	25
E-commerce Fraud (database hacking): unauthorised system access to government & corporate databases, enabling theft of personal information (targeting of individuals of high net worth or specific employees), achieving online authentication for goods/services purchase (particularly financial services).	2.12	26
E-commerce (card not present): online data mining (chat rooms, newsgroup, databases, questionable credit reference agencies) to achieve fraudulent online authentication (targeting of individuals of high net worth or specific employees) & purchase goods/services.	2.37	27
Domestic device account access: the accessing of domestic digital devices (e.g. desktop boxes) through various means to access and copy personal account information by criminals for account hijacking purposes.	2.68	25
Other		
Online professional services: fraudulent investment, banking or other professional service opportunities, achieved by social deception through personalised emails, fake websites, 'investment email' alerts, offshore banks.	2.30	23
Criminal employees: internal fraud (such as procurement or payroll fraud) by unauthorised system access or data disclosure, using various means, by criminal internal employees (or third party insiders) for personal gain.	2.62	26
Online gambling: gambling sites obtain bets for rigged gambling.	2.71	21

[9] http://www.apacs.org.uk/ is the UK trade association of banks and building societies which exchange customer payments.

Card-not-present fraud is a well established form of payment card theft which revolves around an offender's ability to obtain sufficient payment card details to execute fraudulent authentication for online purchase of goods and services. Common forms of card-not-present fraud involve the purchase of goods and services either over the phone or on the Internet. However, as the levels of such fraud have risen websites have increasingly demanded more biographic data to authenticate transactions. This has led to offenders expanding into wider identity theft, where they, to varying degrees, fake the biographic details of the victim to enable them to execute online purchases using payment cards. In obtaining both payment and personal information offenders are becoming increasingly creative and technically sophisticated by such means as creating functioning fake websites. Recent cases have included spoof emails and websites of legitimate banks in an attempt to obtain key account and security details from victims (Symantec, 2003: 1; Silicon.com, 2003:1). Underlying many such frauds, however, is what hackers and IT security specialists call 'social engineering', which relies upon the trusting nature or naivety of many people and their often unhesitating response to give away personal information such as passwords (HumanFirewall, 2002). Respondents identified many potential sources of such information beyond that held in relative security by legitimate holders (from whom it can be stolen by hackers). Sensitive information is increasingly held in personal computing devices such as mobile phones, PDAs and home networks which may be vulnerable to external intrusion or theft. The increasing introduction of chip and pin technology into payment cards will not, however, reduce card-not-present fraud as it seeks to reduce the use of stolen or cloned cards.

Whilst much card-not-present e-commerce fraud actually affects online retailers more than card holders, consumers can also be targeted via the Internet as many other traditional frauds move online. Examples of this are 419 or advance fee fraud, fake investment or other 'get rich' schemes. As with other frauds, such schemes rely upon human weaknesses rather than technological failings. Similarly internal employee fraud involving computer systems continues to be a significant threat, where the problem largely lies with people and process management rather than the computer systems themselves.

Extortion

Extortion is the illegal obtaining of money from a person or organisation by force or threats. Extortion against commercial organisations or individuals is another old crime given new form by the Internet. Commercial organisations may lose money directly through their inability to trade due to impairment of their website via a denial of service attack (preventing customer access to the site) or damage to essential systems such as their customer or product databases (data corruption). Offline organisations may also be threatened by impairment to their operations due to disruption of computer systems which control manufacturing or other industrial operations. Individuals and organisations may also be harmed by the public disclosure of sensitive information which may harm their personal and/ or professional standing, again a traditional form of blackmail. To facilitate any of these crimes, individuals with access to sensitive system information may be targeted as a means to overcome system security.

Table 3.3: Extortion threats

	Score	N=
Service disruption and data breach		
Data corruption: threat of data corruption through various means.	2.69	26
Data corruption of business purchasing & distribution systems: the threat of unauthorised system access to online B2B purchasing portals, to copy/ delete/ modify data and/or deny service.	2.53	19
Automated control systems: threat of unauthorised system access to modify data and disrupt Internet and wireless LAN accessible industrial automated control systems (PLC, DCS, SCADA and MMI).	2.45	20
E-commerce: denial of service threat through various means to disable an online e-commerce sites (B2Cor B2B).	2.34	29
Data disclosure: threat of unauthorised data disclosure through various means (the malicious release of sensitive system data-criminal, medical, financial records).	2.54	26
Methods		
Employee intimidation: unauthorised system access through intimidation or blackmail of employees to achieve various data actions.	2.60	25

Respondents commented that many tools for denial of service and penetration attacks are freely available on the web, with the ability of offenders to disrupt large commercial websites through denial of service attacks and the penetration of systems to obtain sensitive information well documented. In February 2000,

a spate of attacks hit the biggest names in e-commerce — Amazon, eBay and Yahoo (Information Management & Computer Security, 2000). In July 2003, an offender was jailed in the USA for one of the early high profile extortion attempts against a global information provider back in 2000 (BusinessWeek Online, 2003).[10] This offender had successfully penetrated the victim's network, but it was noted by the panel that as with all extortion, only the threat of an attack has to be credible for the offence to work. The threat of disruption to industrial automated controls systems was believed to potentially increase as such systems increasingly move from proprietary closed systems to non-proprietary platforms (e.g. common operating systems) with Internet connectivity.[11] This concern echoes warnings from bodies such as the UK National Infrastructure Security Co-ordination Centre. Such is the recognition of the threat to organisations from online extortion that liability insurance is now available to cover a variety of such incidents.

Espionage

Espionage is the illegal obtaining of information through the use of spies or other means. As with extortion, espionage (commercial or political), against organisations or governments is an old crime given new form by the Internet. Commercial espionage by corporate spies was considered the greatest risk by the panel to commercial organisations, followed by criminal spies, and has been a source of concern to information assurance specialists for a number of years (Information Management and Computer Security, 1999: 1) . The former may work directly for a competitor or third party specialists retained for obtaining 'business intelligence'. The latter may seek out sensitive information on their own initiative and then seek to sell it to a competitor. Political spies undertake both commercial and political espionage to generate a national advantage. Similarly, high profile examples of disaffected employees have been found in both the commercial and government sectors disclosing both commercial and political (military or security service) intelligence. Hacktivists, whose campaign may be against corporations or Governments, may similarly seek out sensitive information from either sector, though the panel considered them the least source of threat.

Table 3.4: Espionage threats

	Score	N=
Espionage source		
Corporate spies	1.89	27
Criminal spies	2.17	29
Political spies	2.24	24
Disaffected employees	2.47	30
Hacktivist	2.54	28
Espionage methods		
Social Engineering: unauthorised disclosure of information through the use of social engineering.	2.17	30
Spyware: unauthorised system access by use of spyware or trojan script.	2.25	32
System penetration: unauthorised disclosure of information through unauthorised system access.	2.32	31
Device theft: unauthorised disclosure of information through the theft of a device e.g. laptop or PDA.	2.4	30
Data intercept: unauthorised disclosure of information through use of a data tap, particularly wireless network.	2.45	31
Employees: unauthorised disclosure of information by employees' for personal gain or emotional reasons.	2.47	30

Respondents commented on both sources and means of espionage. The targeting of sensitive information through the theft of either laptops or PDAs may increase as users increasingly store password details, documents and other corporate information on such insecure devices (see discussion in *Portable communication and computing devices*). In regard to system penetration, respondents particularly flagged the vulnerability posed by wireless networks as they become more widespread. Also the use of various forms of spyware[12], currently largely used for marketing purposes, was identified as a potential hole in computer systems allowing unauthorised data access. Greatest concern, however, was expressed regarding the role of employees in passing information, whatever their motivation. This is a long standing concern widely echoed by other commentators (ComputerWeekly.com, 2003:1). It was noted that the leaking of information is facilitated by low-tech issues such as the absence of adequate internal access

[10] Further details available at http://www.businessweek.com/bwdaily/dnflash/aug2000/nf20000822_308.htm .
[11] For a further discussion of SCADA vulnerabilities see http://documents.iss.net/whitepapers/SCADA.pdf
[12] A detailed explanation of spyware can be found at http://www.pestpatrol.com/pestinfo/.

controls to information and the high street availability of small devices which can store large amounts of data (e.g. USB key rings and digital music players that also record other forms of data).

Malicious software

Malicious software is a broad term that includes viruses, worms, trojans and the increasingly found 'blended threats', which are a combination of more than one previous category of threat. The rise in malicious software has been dramatic, its frequency having increased almost 300 per cent between 2000 and 2003 (MessageLabs, 2003). In one particular source, malicious code was detected in approximately one in every 790 emails during 2000. This rose to one in 380 during 2001, one in 212 during 2002. As of March 2003, impact had stabilised at one infected email per 270 (ibid.).

Table 3.5: Malicious software

	Score	N=
Mobile device disruption: data disclosure or corruption of various devices (e.g. mobile phone, vehicle telematics, digital cameras, PDAs, tablets).	2.08	24
Domestic device disruption: data disclosure or corruption of home devices (e.g. digital television set-top box).	2.35	23

Whilst the existence of such code may continue to represent a challenge, it is clearly not new. However, as the scope and application of computing and networked devices increases, so, respondents fear, will the reach and impact of viruses and worms. As computers enter formerly non-computer based devices, so such devices will be faced with the dangers that have always faced computers such as unauthorised access and data corruption or loss. This can lead to service disruption of the attacked device, or the loss of sensitive data. Potential targets include mobile phones and portable computing devices (Information Management and Computer Security 2001: 3), car-based computers and home networks such as networked entertainment or utility devices.[13] Whilst there is little evidence of mobile phone viruses to date, they have been shown to be vulnerable to received data which can cause them to malfunction (@stake, 2003). Respondents' concerns over the extent of data held in mobile devices has previously been discussed. One potential factor identified in the viability of infecting these devices is the adoption of a common platform across the devices and their manufacturers. As with personal and business computers, the emergence of dominant operating systems brings with it a large target population for virus writers, whilst niche systems are ignored due to their small target population which hinders the spread of any such virus.

Malicious misinformation

This category was not one of the original thirteen used in the survey by panellists. It is composed of items from other categories, including the non-categorised cluster. Its creation reflects another aspect of the focus here on the importance of information as an asset. Along with the primary focus on maintaining its confidentiality, integrity and availability, information (correct or incorrect) can be misused for a number of purposes. The malicious placing of fake information can be driven by a variety of motives including fraud, extortion or dislike of a person or organisation. Attempts to manipulate share prices by distributing misleading information are known as 'pump 'n' dump' (also 'trash and cash') schemes and have existed as far back as 1999 (Information Management and Computer Security, 1999: 2). This threat is explicitly acknowledged by the UK Financial Services Authority (FSA, 2003) and the US Securities and Exchange Commission publishes preventive measures on its website (SEC, 2003).

Table 3.6: Malicious misinformation

	Score	N=
Market manipulation: Distribution of fake information by various platforms (e.g. newsgroup and bulletin postings, email alerts) to manipulate financial services e.g. share price.	2.30	20
Market manipulation: fake websites (authenticating fraudulent data) to manipulate financial services e.g. share price.	2.35	20
Misinformation: distribution of false/misleading information through various platforms (chat, websites, newsgroups).	2.56	32
Extortion: threat of unauthorised system access through various means to modify data (the malicious placing of illegal content on a system).	2.54	26

[13] A discussion of the such disruption can be found at http://www.kaspersky.com/news.html?id=92 .

Such manipulation can vary from merely talking shares up on trading forums by pretending to be multiple contributors or more overt forms of fraud by issuing fake news items from otherwise reliable financial services. Misinformation can be placed for non-financial reasons. Examples of pure mischief making are virus hoax emails, in which recipients are warned of a non-existent virus and advised to remove certain files from their computer.[14] Other examples include those targeted against individuals such as celebrities which are little more than malicious gossip. Such is the extent of the problem that websites and newsgroups exist which track such misinformation.[15] Another form of misinformation, flagged up as a form of extortion, though it could occur without an extortion demand, is the 'framing' of an individual by the remote placement of illegal or otherwise harmful content on their computer. This could be achieved through various means and it has already been used as successful grounds for defence for an individual charged with possession of paedophile content (ZDNet, 2003:1).

Unlawful markets and dangerous communities

As with the malicious misinformation category, this category was not one of the original thirteen used in the survey by panellists and is composed of items from the non-categorised cluster. Its creation reflects the phenomenal capability of the Internet to distribute information and allow people to form communities of common interests. Such communities of interest, as well as commercial operations can use the Internet and various platforms (websites, peer-to-peer applications) for an infinite number of legal and illegal purposes.

In business terms the Internet represents another route to market or means of distribution. For criminals this is equally true and auctions websites have joined 'second hand shops' as a means of fencing or passing on stolen goods.[16] One panel member had experience of an item being advertised for sale although the victim was still in possession of it – the item would have been stolen to order once it had been sold via the Internet. A unique benefit of the Internet for legal retailers is they are able to easily reach a global market. This represents problems, however, when local laws that vary from country to country regulate the product or service in question.

Table 3.7: Unlawful markets and communities

	Score	N=
Portals: victim and offender aggregation (e.g. paedophiles)	1.76	17
Black market sales: increased access to purchasers of unlawful products & services (e.g. unlicensed pharmaceuticals) through various means (websites, newsgroups, chat rooms). Undertaken by unethical companies for commercial advantage (grey market distribution) or criminals for personal gain.	2.28	29
Online fencing: increased access to potential purchasers of stolen products through various means (websites, newsgroups, chat rooms).	2.46	28

Respondents flagged the pharmaceutical industry as a prime example of this where prescription only or non-UK approved drugs are available to consumers from retailers in countries where no prescription is required, thus circumventing UK laws.[17] Early examples of this include Viagra and various steroids (BBC Online, 2000). A related problem is the sale of fraudulent products, again often health related. This is an area regularly investigated by the UK Office of Fair Trading.[18] Respondents noted pharmaceuticals as an area of particularly high risk for this activity and pointed out that in light of increased regulation of public websites, markets will move to more closed channels such as chat rooms and newsgroups. Other examples of concern are the sales of weapons and weapon re-activation components outlawed in the UK but available from overseas (NCIS, 2003). More broadly the ability of the Internet to bring individuals together, whatever their shared interest, has been recognised as an enabler of offending communities, the best documented example being paedophiles. Sophisticated Internet-based platforms for the forming of communities, legal or otherwise, are readily available through global portals[19] and allow file sharing, postings, chat and relative security by member only access.

[14] Examples of such hoaxes can be found on various anti-virus websites (e.g. http://www.symantec.com/avcenter/hoax.html)
[15] An example of such as site is http://www.truthorfiction.com/.
[16] For examples see http://www.auctionbytes.com/cab/abn/y03/m01/i06/s02 or http://www.siliconvalley.com/mld/siliconvalley/3443962.htm.
[17] For examples of online pharmaceutical purchasing see http://observer.guardian.co.uk/uk_news/story/0,6903,1015849,00.html
[18] For details of the Office of Fair Trading work in this area visit http://www.oft.gov.uk/news/press+releases/2002/pn+14-02.htm
[19] Examples include Yahoo Groups (http://uk.groups.yahoo.com/).

As well as helping offenders share information and normalise their aberrant behaviour, community platforms also bring offenders into contact with victims. Paedophiles and various fraudsters are to be found looking for victims in community groups, chat rooms and newsgroups. Most such environments are not monitored in any way, representing (particularly for children), the convergence of offenders and victims in the absence of a capable guardian (Felson, 1998).

4. Technology challenges

The previous chapter sought to examine the first objective of the study: identifying what areas of Internet and information technology application will be the possible focus of criminal activity in three to five years time? This chapter examines objective two: what areas of Internet and information technology possess the potential to be misused by criminals and represent a challenge to law enforcement. The use of the term challenge reflects the fact that such technologies are not illegal, and in many cases are in fact very positive drivers for change in society e.g. broadband. However, as with almost all technology, there is the potential to facilitate criminal activity. In discussing these concerns, the challenges will be discussed in terms of the risk they present to the immediate user, risks to the service provider (e.g. telecommunications or ISP company), or how they may more broadly facilitate the execution of crimes.

Broadband

Broadband is a general term for a variety of technologies that connect a computer to the Internet at a rate of between 150Kbps and above.[20] At the end of July 2003 there were just over 2,443,500 UK broadband subscribers, with approximately 30,000 connections every week. Of the 47 per cent of UK homes connected to the Internet at the end of May 2003, approximately 15 per cent do so with a broadband service. For UK small and medium businesses, of the 65 per cent who are connected to the Internet, approximately 24 per cent do so with a broadband service (Oftel, 2003). The Government is seeking to promote the uptake of broadband by considering encouraging new homes and buildings to be built in such a way as to make it easier to distribute computer cables.[21]

Table 4.1: Broadband

	Score	N=
User vulnerability		
Personal data for identify theft: identity theft following a hacking attack to access personal details.	1.88	24
Service theft (storage): theft of disk space following an attack to store illegal material on a home computer without detection.	2.38	26
Illicit secretion of material: hack of home computer to store illegal material on a computer.	2.43	23
Data theft or copying: hack of home computers to 'steal' music, movie files or other content.	3.13	24
Misuse facilitation		
Facilitate peer-to-peer platforms: faster, always on nodes will increase use of peer-to-peer links.	1.95	22
Service theft: attacks on insecure home machines giving intruders control of very large bandwidth and cpu resources for denial of service attacks.	2.00	26
Facilitate rapid illicit data transfer for remote storage	2.08	24

Broadband is significantly faster than the traditional dial-up Internet access over telephone lines. A faster speed makes the downloading (and uploading) of large files (e.g. images, video, music and software) convenient and affordable. As the technology allows the telephone line free for calls and is not charged by the minute, users are able to leave their computer permanently on and connected to the Internet. This permanent connection to the Internet, coupled with the poor security adopted by most users (NCSA, 2003) leaves them vulnerable to being hacked, something traditionally associated with large non-domestic computer systems. Such unauthorised access could be motivated by targeted maliciousness (e.g. the inserting of illegal content onto someone's computer), the gathering of personal information for identity theft, or a non-personalised attempt to take over a machine to use in an attack (e.g. a denial of service) against a third party computer. Compromised home computers could also be used to store material, often illegal, something frequently found with larger commercial or university systems.

[20] A simple overview of broadband is provided by Ofcom at http://www.ofcom.org.uk/research/consumer_audience_research/telecoms/wireless_update/wirelessbroadband/Section3?a=87101

[21] (Building Regulation and Electronic Communications Services (Broadband) consultation exercise, Office of the Deputy Prime Minister, 2003).

Such dangers are exacerbated by risky behaviour such as using peer-to-peer file sharing programs or downloading files from unknown senders. Dial-up Internet users are exposed to similar risks but to a lesser extent.

More broadly, quicker upload and download times have facilitated the dissemination of content, much of it illegal, such as pornographic images and pirated software and music. The rise in dissemination has been equally driven by the development and popularity of peer-to-peer applications, which are discussed in the next section. Such rapid uploading and downloading may also encourage the remote storage of large data sets (e.g. paedophile image collections) outside the home (this issue is discussed later) to avoid detection from law enforcement if a computer is seized.

Peer-to-peer platforms

Peer-to-peer (often written as P2P) communication occurs in its purest form when two computers communicate without going through a third computer (i.e. server). However, many peer-to-peer products use a hybrid approach that can incorporate a server. Users are normally required to install the same networking program (e.g. KaZaA) to connect with each other and directly access files from one another's hard drives.[22]

Table 4.2: Peer-to-peer platforms

	Score	N=
User vulnerability		
System penetration: trojan horse functionality in file sharing clients – possible utilisation in DDoS attacks, unauthorised data disclosure.	1.83	18
Misuse facilitation		
Covert means of communication by serious criminals & terrorists.	1.70	20
Covert distribution and storage: distribution of indecent and offensive material.	1.71	21
Covert distribution and storage: distribution of pirated copyright material.	1.96	26

Respondents noted the increasing role of peer-to-peer platforms as a means of distributing illegal content, such as pornography, paedophilia and perhaps, most commonly, for pirated material such as music. This concern is shared by other recent research (GAO, 2003). As most peer-to-peer software is free it frequently contains explicit or covert advertising related software. Some of this software may contain various forms of spyware or other software which may send sensitive information about the user and his/her Internet behaviour to a third party. In addition, it may allow a malicious third party access to the computer.[23] A number of Internet worms and viruses are spread through the use of popular peer-to-peer applications such as KaZaA and Morpheus (Symantec, 2003:2). Ultimately, the use of applications such as peer-to-peer applications may represent present legal liability for individuals and corporations if used inappropriately or otherwise enables a security breach.[24] Peer-to-peer code is now found in many Internet worms (such as Slapper[25]) which use it as a covert means of taking control of infected machines in preparation for subsequent activities such as denial-of-service attacks on third party machines.

Portable communication and computing devices

Mobile phones are in common use today, as are the use of small handheld computers, colloquially known as personal digital assistants, both representing vulnerabilities alongside the benefits they may bring. Such devices are able to hold not just diary information but word and spreadsheet files, as well as small databases. As these devices take a place alongside corporate laptop computers they add a new risk dimension to that already posed by mobile computing (Information Management and Computer Security, 2001:4).

[22] A more detailed definition of peer-to-peer technology can be found at http://searchnetworking.techtarget.com/.
[23] A detailed discussion of the security dangers of P2P platforms can be found at http://documents.iss.net/whitepapers/X-Force_P2P.pdf .
[24] A detailed explanation of the vulnerabilities of peer-to-peer applications such as KaZaA can be found at http://www.hpl.hp.com/shl/papers/kazaa/.
[25] For details of the Slapper worm see here http://www.crime-research.org/eng/news/2002/09/Mess1701.htm.

Table 4.3: Portable communication and data devices

	Score	N=
User vulnerability		
Identity theft: information contained in mobile phones & PDAs facilitates unauthorised disclosure of personal information.	1.96	25
Stalking, harassment: personal devices with GPS provides means of tracking or threatening to track individuals e.g. paedophiles and young children.	2.40	15
Data theft: data tap on mobile communication devices.	2.54	13
Service provider vulnerability		
Mobile communications service theft: reprogramming of chips/SIM cards/IMEI numbers to obtain free services.	2.31	16
Mobile communications service theft: network hack to obtain free services.	2.42	12
Mobile communication distributed denial of service: service disruption by SMS (text).	2.64	11
Mobile communication denial of service: service disruption by service jamming.	3.18	11
Misuse facilitation		
Anonymous communications: user anonymity for criminals, terrorists via unregistered phones.	1.88	25
Image distribution: distribution of pornography.	2.10	21
Espionage: data theft via photo phones & portable storage devices.	2.22	18
Mobile data transfer: data and imaging capability of mobile phones & pda devices (e.g. To organise and manage riots).	2.39	18

Research has indicated that a significant number of people use portable devices to hold both sensitive personal data (bank account details and PIN numbers) and work information including corporate information and passwords (PointSec, 2003). Research has also highlighted the lack of secure authentication that currently protects such information if the device is lost or stolen, despite users being potentially open to more security measures (Clarke *et al*., 2002). As the network capability of such devices increases, such as wireless networking, they are increasingly used to access work networks directly to upload and download information. Forty-one per cent of such networked users bypass the password function when accessing their work network. Such information is highly vulnerable if stolen by offenders, as half of users do not encrypt stored work data (ibid.). One in four users lose such PDAs, many holding unprotected sensitive personal and work information. Of even greater concern is the convergence of such devices with mobile phones, as 40 per cent of users have lost their phone (ibid.). Smartphones which combine PDA functions are now able to receive and store emails and files through various means (e.g. normal telephone transmission, infra red and Bluetooth). Such devices have existed for a number of years but their use is set to increase dramatically (ARC Group, 2003: 1). Such concerns take a concrete form when considering the current deployment of such devices in a UK nuclear facility (ComputerWeekly, 2003: 2). The data held in such devices can be disclosed through their accidental loss, their deliberate theft and the penetration of the devices by wireless means.[26] The devices have also been susceptible to viruses for some time (Information Management and Computer Security, 2001: 3).

Both mobile phones and PDAs are now available with digital cameras and will become more widespread as their price drops and networks services increase. It is estimated that around 25 million camera phones were sold worldwide during 2002 and that this figure could increase to 55 million during 2003 (Silicom.com, 2003:2). Respondents flagged concerns over the use of such devices for espionage and invasions of privacy (evidence not to be found on your person if immediately transmitted and deleted) or criminal orchestration (e.g. send photographic evidence of kidnap victim whilst on the move). Already there are reports of industrial organisations banning the presence of such devices from sensitive research facilities to prevent commercial espionage (Silicon.com, 2003:3) and the UK leisure industry has been issued guidance on preventing the use of mobile phone cameras in leisure centres to prevent the photographing of children and other invasions of privacy (ISRM, 2003). One UK local authority has already banned the carrying of mobile phones in its leisure facilities (Guardian Online, 2003). The use of photo mobile phones

[26] Many advanced phones can talk to other devices (phones, PDAs, computers, printers) via the Bluetooth wireless protocol. At least one tool has been developed which interrogates nearby phones and can read device information if Bluetooth is enabled.

to capture and or distribute illegal images was highlighted by respondents in terms of the image transfer capability of such devices in discussing technology challenges, but also when specifically discussing the criminal threat of online paedophile image trading via GPRS[27] mobile phone as a criminal threat. There have already been reports of such use by UK offenders (Sunday Mail, 2003).

Although crude location tracking is possible with current mobile phones, the next generation of 3G phones provide location identification possible to an accuracy of around ten metres by utilising global positioning systems (GPS) technology. Commercial services which enable the tracking of individual mobile phones to any member of the public now exist. Whilst such services claim to control unauthorised tracking, the fear that they can be located, as with the fear behind extortion, may be sufficient grounds for harassment for users, particularly children. In mid-2003 it was estimated that around 400,000 children under the age of ten have their own mobile phone, following trends seen in other countries with advanced mobile phone services (mobileYouth, 2003).

Increasingly advanced communication and computing devices represent vulnerabilities not only to their users but also to those who provide them, the service providers. Respondents stated that service disruption could be caused by jamming the network or overloading elements of it with text messages. Although the disruption of SMS text service may not appear significant, UK companies are increasingly using text messages to communicate essential information (Silicon, 2003: 2). Such attacks could be against specific individuals or against a specific operator if telephone number blocks were targeted. Examples of mobile phone disruption by text have already occurred, such as the Timofonica worm in 2000.[28]

Wireless networks

Wireless networks are computer networks that carry data over a radio signal rather than a physical medium such as electrical or fibre optic cabling. Although not a new technology, the recent upsurge in its use has been the result of the emergence of joint industry standards (IEEE 802.11), sometimes also referred to also as Wi-Fi.[29] The adoption of a single standards framework has led to the rapid roll-out of hardware that has enabled the dramatic rise of wireless network deployment in commercial, home and even personal settings. To enable more flexible work practices, organisations may use wireless networks to allow staff to work at almost any location when equipped with a wireless-connected laptop computer or other device. As computers increasingly enter the home, users are buying small wireless kits which allow them to similarly work from any room or the garden with a wireless computer. Wireless technology for home users may be particularly popular as a means of bringing broadband connectivity to areas where the physical cabling infrastructure is not in place.

Table 4.4: Wireless networks

	Score	N=
User vulnerability		
Home networks: nuisance attacks against household systems by penetrating home-based wireless networked system.	2.44	18
Service provider vulnerability		
Service theft: theft of service (bandwidth) by tapping into wireless network and using for transmitting data.	2.00	17
Denial of service attack: system attacks via wireless transmission	2.47	15
Data breach: unauthorised interception of network traffic.	3.17	18
Misuse facilitation		
Mobile offenders	2.06	16

Another wireless technology is known as Bluetooth,[30] used to connect small scale devices in close proximity to each other (e.g. a laptop computer and a nearby printer). As highlighted earlier there is now an increasing convergence between mobile phones and small computers, and such devices are often able to talk to each other and nearby networks and devices using either Wi-Fi or Bluetooth technology; such scenarios are sometimes called Personal Area Networks.[31]

27 General Packet Radio Service (GPRS) is a digital mobile phone technology that enables the relatively slow transfer of files (e.g. photos).
[28] For further details see http://www.kaspersky.com/news.html?id=67 and http://news.zdnet.co.uk/hardware/mobile/0,39020360,2132143,00.htm.
[29] For further information on Wi-Fi networks see http://www.wi-fi.org/ and http://www.wikipedia.org/wiki/Wireless_network.
[30] For further information on the Bluetooth protocol see https://www.bluetooth.org/
[31] For further information see http://en.wikipedia.org/wiki/Personal_area_network

As with the roll-out of broadband technology, wireless networks[32] bring vulnerabilities as well as benefits to both their users and their service providers (*Computers and Security*, 2002:1; 2). For wireless networks the primary vulnerability is that the network, and hence the data it transmits, can be accessed without an offender achieving physical access to computers or cabling. So, equipped with a wireless receiving and transmitting computer, an eavesdropper would be able to stand outside a building which is using a wireless network and physically intercept the signal. Previously they would have had to obtain physical access to the building or connect to the computer network remotely via a physical telecommunication network. Wireless networks are easy to detect (the searching out wireless networks is known as 'wardriving') and, currently, relatively insecure.

Public, though often for a fee, wireless access points are also rapidly appearing in locations such as coffee shops, conference centres, hotels and airport lounges. Such locations offer offenders both increased mobility and a convenient source of potentially vulnerable users whom they may hack, reducing even the need for wardriving as a means to intercept mobile commercial workers.

As well as concerns over unauthorised data disclosure, respondents highlighted the potential for home network disruption by hijacking domestic wireless networks which link up devices. Although in their infancy, home networks and automated systems[33] are not new. Currently based around entertainment systems, future applications could include networked appliances (e.g. the Internet connected microwave, fridge or central heating). Other unauthorised access concerns included commercial spammers. Commercial spammers are well known for unlawfully using the networks of innocent third parties to distribute their material as it saves them money, and more importantly, disguises their identity (as the violated third party gets the blame as the originating source of the spam mail). System administrators have become aware of this and now largely secure access to the email elements of their network. Wireless networks, however, now represent a new way into a third party network which can enable spammers to continue to steal service capacity (e.g. network bandwidth to send the emails). This practice is called 'warspamming'. As discussed, one of the key drivers of wireless networks is the mobility they give users and this of course also goes for offenders. Respondents noted this potential in the context of the mobile wireless transmission of paedophile abuse. However, such mobility could be used for any illegal or malicious activity, particularly if used with public access wireless access points that do not require a subscription or collect an IP address (ZDNet, 2003:2).

Anonymity, havens and counter forensic services

The achievement of anonymity and other forms of privacy were a strong part of the early Internet community ethos and still remain strong in many areas today, alongside traditional offline privacy concerns. A number of diverse concerns were identified, all of which revolve around the forms of anonymity that can be abused to facilitate criminal activity.

Table 4.5: Anonymity, havens and counter-forensic services

	Score	N=
Misuse facilitation		
Forensic evidence eliminators: cleaning out PCs of incriminating materials e.g. Paedophiles.	1.88	24
Anonymous communications: lack of authentication required for Internet café and kiosk services.	2.04	23
Anonymous communications: via open mail relay & anonymisation services: secure illegal communications (content or intent).	2.12	25
Offshore hosting: offshore hosting for safe 'dead drop' storage of illicit data.	2.16	19
Anonymous communications: anonymising services from service providers.	2.41	17

Internet users can achieve various degrees of anonymity whilst either surfing the Internet or sending emails. Whilst some means may require significant technical knowledge (e.g. using open mail relays), others are available to anyone using dedicated website-based services (anonymous remailers[34]). Alternatively and perhaps most simply a degree of anonymity (though location may be identified) can be achieved by using an Internet café or street email kiosk. Respondents also specifically cited the use, authorised or otherwise, of wireless networks as a means of offenders using the Internet anonymously. If

[32] For a discussion of wireless broadband access see http://www.ofcom.org.uk/research/consumer_audience_research/telecoms/wireless_update/wirelessbroadband
[33] A further discussion on home networks and automation can be found at http://www.intel.com/labs/commnet/homenet.htm?sfgdata=4.
[34] A discussion of anonymous remailers can be found at http://governmentsecurity.org/articles/Whatisananonymousremailer.php

an offender is able to access the Internet via unauthorised access to someone else's wireless network (e.g. a home or business wireless network which then connects to the Internet via an ISP) then he/she may in fact be hiding behind someone else's identity, rather than being truly anonymous. Alternatively, if they access the Internet via a free public wireless access point then, although the rough location could be identified, no individual could be identified as no log-on or IP details may exist. The source and strength of the anonymity varies in each scenario but most represent a challenge to the bulk of normal policing investigations.

As well as anonymous communications, offenders may require secure storage for sensitive data for fear of its seizure, such as paedophile content, sensitive financial records or material illegally obtained. Although the much talked about concept of data havens may be considered somewhat exaggerated, similar services do exist.[35] Personal computers in the home or workplace can betray both personal content (even once deleted from the machine) and Internet surfing history. To securely remove such information, specialist software can be purchased in the high street that will attempt to 'scrub' computer disks of any evidential remnants. The use of such tools may increase as the tools become simpler and offenders more forensically aware, a pattern seen in other forms of criminality (e.g. the use of condoms by rapists).

Authentication mechanisms

In computing terms, authentication is the process by which a computer or another user attempts to confirm that the computer, or user from whom they have received some communication (or are presented with in physical terms) is, or is not, who they claim to be. In the physical context, the use of biometric recognition systems, such as iris or fingerprint readers are increasingly being used in applications such as credit card verification and airport check-in.

Table 4.6: Authentication mechanisms

	Score	N=
Service disruption/ user vulnerability		
Identification systems including smartcards: false documentation used to further illegal activity e.g. Fraud.	1.62	13
Biometric applications (data corruption): alter or delete data to compromise legitimate identification.	2.42	12
Biometric applications (data secretion): implant data to generate false identities.	2.57	14

Systems invariably rely upon a computer database which holds details of authorised users. Respondents noted that if such a database was corrupted or rendered unavailable the system would fail, causing potentially significant disruption. Such disruption could be against a particular authorised user or the whole service. Alternatively offenders seeking to obtain access to a location or information via a biometric device have two options. Either they try to authenticate as somebody else, by having to mimic their physical characteristics by some means, or they legitimately authenticate to an identity illegitimately added to the database. This latter method is flagged by respondents, noting that once entered into a database considered secure, the attacker would be rendered a 'trusted source'.

Another identification and authentication issue related to the increasing use of smartcards is that smartcards resemble a credit card but store their data in a microprocessor chip rather than the traditional magnetic strip. The microprocessor enhances the card's security by seeking to control access to the data it contains by interacting with any computer that seeks to read it.[36] The forthcoming 'chip and pin' payment cards are a form of smartcard, as are the cards found in satellite or cable access television receivers. However, such systems could be subverted through the production of fake cards, rather than an attack on the database system itself. Smartcards have been used in numerous applications and have a history of being faked or hacked.

Data mining

Data mining is the automated searching of large data stores for patterns, or in the context discussed here, specific pieces of information. The Internet may be considered the largest and most accessible repository of information ever known and continues to grow, supplemented with commercial and non-commercial databases, as well as the ever changing and largely transitory 'data noise' generated in a million newsgroups and chat rooms.

[35] An example of secure anonymous storage services would be LockBox (www.lockbox.com), which provides 'a secure web-based system for transmission of confidential or sensitive documents for business or personal application'.
[36] More information regarding smartcards can be found at http://electronics.howstuffworks.com/question332.htm.

Table 4.7: Data mining

	Score	N=
Neural networks and data mining techniques of open online information sources to achieve unauthorised system access with acquired public information.	2.54	13

Respondents noted that the number of systems that can be accessed to find out personal information from open sources is a boon to investigators but can equally be used to 'target' individuals. Information gathering can be used to facilitate offences such as identity theft and espionage. Such activity may use public search engines, or bespoke or specialised software tools. Also, as noted by some respondents, offenders may use online 'credit reference agencies' whose *bona fides* they found questionable. Although not cited by respondents, information could also be gathered to facilitate the online stalking of individuals, particularly if they participate in online forums such as chat rooms or newsgroups.

5. Summary and recommendations

Summary

This research set out to identify a body of opinion that could consider criminal and anti-social opportunities that may derive from future developments in computing and Internet technology. Such a panel was successfully assembled, encompassing a diverse body of knowledge, experience and competence. The panel diversity was reflected in the scope of the criminal threats and technology challenges put forward. A hundred and one threats over a broad range of offences were identified. Although the threats were very close in respondents' threat ratings, the top ten threats (see Appendix A) covered online paedophilia, espionage, fraud and piracy. Although seven of the ten were related to online paedophilia, this topic is not discussed in the report, along with a number of other threats, on the grounds that priority was given to threats that were generally less documented and identified. The problem of online paedophilia is publicly recognised and documented by law enforcement, government and ISPs with action being undertaken (respondent recommendation to further tackle this problem will be discussed in *The future of netcrime now: Part 2 – responses*). Indeed one may consider if the high media profile given to online paedophilia in any way influenced the prioritisation given to it by the members of the panel, despite their differing disciplines and roles.

One hundred and thirty seven technology challenges were put forward. As with criminal threats, the challenges were very close in respondents threat ratings. The top ten challenges (see Appendix B) covered the use of encryption techniques for secure communications by offenders, peer-to-peer platforms, offender and victim aggregation through online community portals and concerns over the abuse of authentication mechanisms such as smartcards. Of these, cryptography, along with a number of other challenges, was not specifically discussed, again on the grounds that priority was given to challenges that were generally less documented and identified.

Although a number of contributions reflected current concerns, such as fraud or computer hacking, the detail of the contributions was rewarding, despite the limited space given to respondents to document their concerns. For instance, numerous specific forms of fraud were put forward, reflecting both new technologies, as well as societal developments in the provision of goods and services (e.g. fraudulent implications for the roll-out of smartcards and online government services). Responses also reflected the multifaceted nature of much risk. Some risk lay with the goods or service user (e.g. chat room), some with the service provider (e.g. online merchants are also major victims of e-commerce fraud) and, some with those targeted by offenders using technology to offend (e.g. victims of confidence-based frauds such as 419 fraud).

In discussing victims of netcrime, the research findings illustrate the variable nature of their targeting by offenders. Newman and Clarke's (2003) target categories explicitly distinguish between *primary*, *transitional* and *convertible* targets which encourages one to look beyond the immediate offence or behaviour (e.g. hacking into a network) and consider the offender motivation and wider target (e.g. fraud, espionage, extortion or thrill seeker). A deeper understanding of such targeting and possible motivation is also made possible when one understands that in some offences the victim may be specifically targeted (an *attractive* target), largely the product of opportunity (e.g. a *proximate* target chosen because a network scan found a vulnerability) or merely an unfortunate *undifferentiated* victim of random offending behaviour (e.g. a virus victim). The criminogenic potential of technology or products has long been discussed in regard to its misuse by offenders and this is reflected in the research responses. Technology can facilitate criminal activity when used in accordance with its explicit purpose, for example the use of innocuous camera phones to invade individuals privacy or to overcome measures aimed at stopping paedophiles photographing children. Some technology can be used in ways that it was not designed for with no modification by offenders. Certain digital personal music devices can be used to copy and hold large amounts of data (motivated by espionage or copyright breach) of a non-entertainment format, an application outside its stated function. Similarly, many network monitoring tools designed to assist system administrators are basic tools for computer hackers. Technology can also be modified or created from scratch by offenders with no purpose other than malicious intent. Examples would include the hacking (modification) of smartcards (for a variety of purposes) or the creation of virus kits and viruses. As well as identifying potential problems, the research sought to highlight potential measures to tackle them. Here the panel was equally diverse and broad in its scope. However, these measures are discussed in the second publication from this research, *The future of netcrime now: Part 2 – responses* (Morris, 2004).

Limitations

There are of course limitations to the findings, due to the nature of the topic and the passage of time. As stated at the outset, any futures work is but a 'best efforts' attempt at insight to what may occur. The Delphi method used here is based not on statistical extrapolation but rests on the informed judgement of its participants who are clearly not infallible, nor the sole holders of relevant knowledge and experience. The scope and complexity of the topics on which their views were sought is extreme and highly dynamic, and these findings are but a snapshot of opinions at the time of the survey. If crime prevention knowledge is considered a depreciating asset, as criminals adapt to counter-measures, then any futures oriented warning and information this paper seeks to provide will depreciate faster than most such publications due to the rapid development and application of the technology discussed. Even whilst conducting this survey, a number of items that appeared new and original in the first data collection round, were subsequently reported in technical journals and some offences even made their way to court.[37] This is an understandable product of the panel members' knowledge deriving from ongoing experience in tackling various issues. Omitted from the panel, though an unsuccessful effort was made to identify potential such individuals, were suitable futurologists, individuals whose primary professional role is to consider future changes in technology or societal issues, albeit not from a criminal perspective. The inclusion of such views may have generated some particularly novel suggestions and it would have been interesting to observe the views of the other panel members with more current but security- or crime-based perspectives.

Despite the diverse and often interconnectedness of many of the threats and challenges that have been highlighted by the research, this complexity should not obscure the fact that much of what is seen is merely old crimes committed in new ways. Human motivations, needs and frailties are relatively consistent. Criminals and offenders are largely driven by finding ways of making money which invariably feed upon victims'greed (e.g. 419 fraud), naivety (e.g. online investment scams) or simple carelessness (no or poor use of passwords and other measures to secure computers and other devices). Offenders will always need ways to come into contact with victims or accomplices, preferably in the absence of any kind of regulatory or law enforcement presence (e.g. paedophiles seeking out children or thieves seeking buyers of stolen or otherwise illicit goods or services). Some new crimes such as computer hacking and denial of service attacks, may not be so new if they are committed for the old motives of financial or political gain (e.g. espionage, extortion, hacktivism) or an often juvenile desire for peer recognition and status; a large number of successful young offenders are caught because of their post-offence boasting in chat rooms.[38] Experienced law enforcement or regulatory agents will recognise such similarities quickly enough when they see the potential of these technologies to assist their work and redeploy the resources to take advantage of them.

Notwithstanding viewing much netcrime as merely a new *modus operandi* for offenders, it cannot be denied that a fundamental development in criminal opportunity is occurring. Computers continue to become cheaper, more powerful and ever more present in UK homes. A drop in the price and an increase in the speed of Internet access closely follow this trend. Increased computing power and Internet connectivity are two factors that continue to drive the commercial development of the worldwide web, with an increasing number of goods and services online (e.g. banking, gambling, shopping and government services). Thus we are faced with an increasingly populated online environment, representing a growing pool of victims and offenders. This growing population is being joined by a new wave of emerging technologies. Powerful computers and fast Internet connections are now enhanced by peer-to-peer applications that cut through the chaos of the Internet and directly connect providers and consumers to a variety of legal and illegal content. Such a many-to-many distribution model is powerful beyond any kind of offline equivalent – and is largely free. Beyond the rapid growth of home and workplace computing and connectivity, another driver of criminal opportunity is emerging. As with the computer, mobile phones have become commonplace due to their drop in price and self-sustaining value to users as more people use them. Behind mobile phones, digital devices such as cameras, music players and personal organisers have become more powerful, smaller and cheaper. Functional convergence is occurring here as these functions are increasingly found in a single device. Until recently we possessed powerful computing and Internet connectivity at home, and compact, flexible digital data devices on the move. Now these two clusters of technology development have been combined with a third. Wireless networks, whilst of less immediate impact to most users, can link all these technologies and will pave the way for an increase in the popularity and functionality of a new generation of combined computing and communication devices (e.g. a personal organiser that is a mobile phone, tells you where you are on a map at any time, connects

[37] Hence the title of the report(s), the once future forms of offending are already with us.
[38] See the conviction of Mafiaboy http://news.bbc.co.uk/1/hi/world/americas/1125143.stm.

to the Internet for online banking, talks to your work computer system and is able to pay for services at certain machines with e-money).

Every technological development discussed has to varying degrees been a source of criminal opportunity, be it as target or facilitator of criminal or malicious activity. Increasingly, however, we are seeing the compounding of criminal opportunity as technologies converge. The growths in broadband connectivity coupled with peer-to-peer platforms have each driven the other in facilitating the distribution of pirated material. Similarly, we are on the verge of broadband type connectivity for the next generation of mobile phones coupled with new forms of content distribution via photo phones with colour screens (the new platform); the possibility that criminal or malicious content might be distributed with this technology has been alluded to by the panel; similarly, wireless public networks (connectivity) coupled with wireless-enabled handheld computers, another new platform. Each of these developments represents both a benefit to users and an opportunity to criminals. In looking forward, one will have to consider them not alone, but in conjunction.

Recommendations

Although specific response recommendations stemming from these threats and challenges will be the basis of *The future of netcrime now: Part 2 – responses* (Morris, 2004), it is advisable that a number of stakeholders are made aware of the specific findings of this report so as to consider their own detailed responses. As already stated, many stakeholders will be aware of many of these issues; it is hoped however, that this report contains some that are new to them, along with novel ways of considering offences using frameworks such as Newman and Clarkes' target categories, along with the unpredictable compounding impact of technology developments.

More broadly it is hoped that this research illustrates the potential value of futures research in the area of netcrime, whatever the specific methodology used. The limited product life of such research, however, requires that it be repeated on a regular basis and it is hoped that this challenge is taken up by policy makers, law enforcement and the research community. Earlier crime prevention work discussing the designing out of crime shows great prescience in providing insights in to how we might proceed in this area. Ekblom (1997) talks of the "protracted co-evolution of conflicting parties against a background of incidental disturbances which from time to time give the edge to offenders or defenders [e.g. law enforcement]". One of the major sources of the 'disturbances' he is referring to is the emergence of new technology, products or services that lead to unforeseen criminal consequences as, to varying degrees, offenders adapt their efforts. The combination of the Internet and global retailing now paves the way for such rapid and wide dissemination of new technology that unpredictable negative consequences do not just locally emerge but often explode onto the global environment. Such a rapid emergence of new criminal tools or opportunities can lead to what has been termed a 'crime harvest', as offenders reap the new found criminal opportunity before it is closed. This problem is well illustrated by the continual game of 'catch up' software vendors face as hackers exploit vulnerabilities in their products before a vendor patch is released and implemented – or not – by the software users. The lag between offender first move and defender response is what one must seek to reduce or even close. Unfortunately, in terms of software vulnerabilities, the lag is moving in the offenders' favour, as the time delay between the discovery of a vulnerability (by various sources) and its exploitation by offenders is narrowing, giving less time for the vendor to produce and distribute the patch. What is one to do in light of the increasingly complex and rapid development of information and communications technology which is often accompanied by criminal opportunities?

One of the primary points of the designing out crime literature is the reduction of vulnerabilities by building secure systems at the outset. There is an extensive body of literature in this area which will not be discussed here except to say that it calls for the consideration of security issues, or user misuse, to be a fundamental design criteria at the outset, rather than security considerations being a 'bolt-on' afterthought. Ekblom calls upon defenders to "gear up" to help methods of "prevention by design to evolve as fast as methods of offending, in the face of a stream of new opportunities for crime" (1997). Defenders must react quicker, or indeed be proactive, to reduce or prevent windows of criminal opportunity emerging with new technology and applications. To do this he calls for the need to set up an "infrastructure to speed up the feeding of information on crime and prevention to designers" (1997). In the netcrime context, information needs to flow to not just the designers of new products but also the vendors and users of current products. Such a process may be considered to operate at a tactical level, as it is essentially reactive to each threat. Such a requirement is again illustrated by the large and diverse infrastructure that currently exists to

provide many computer users with warnings and solutions against hacking and virus threats.[39] But what of the numerous other diverse threats and risks raised by the research?

Organisations such as online banks are only recently getting to grips with how they inform their users of threats such as the use of fake emails and bank websites. They, along with numerous other providers of online goods and services, need to review the security of their offerings, the secure practice information they give customers, and put in place rapid response measures when a vulnerability of some kind is exploited by adaptive criminals. Such a strategic review requires a consideration of service or product design and organisational response. Futures research or environmental scanning, whatever form it takes, can inform such reviews. Whilst large software vendors, specialist information security providers or large corporate users may undertake such exercises, this is certainly a space that should be occupied by government and law enforcement and there is already evidence of this. The UK Government's Foresight program[40] has existed for a number of years and is currently undertaking work in the area of cyber trust and crime prevention. This is a broad ranging work which, like this research, has sought to engage a broad community of informed and interested parties in a debate around a number of key issues. More specific to UK law enforcement, two initiatives stand out as potentially relevant. In looking at criminal and technological threats, the National Hi-Tech Crime Unit (NHTCU) produces the annual hi-tech element of the National Criminal Intelligence Service's UK Threat Assessment. Also, the Home Office has convened a programme of work under the auspices of a Police Science and Technology Strategy Group to ensure the police service is equipped to 'exploit the opportunities in science and technology to deliver effective policing as part of a modern and respected criminal justice system'. This program covers the full gamut of policing requirements though there is but one capability specifically allocated to tackling hi-tech crime. The ensuing report to these findings will discuss in great detail the implications for this program of work in regard to tackling hi-tech crime, not just a stand-alone topic but as a function of general policing.

In conclusion, these findings highlight the point that technological and societal changes do have potentially major implications for crime and crime prevention. The arguable difference with netcrime is the speed, complexity and perpetual nature of such change. The continuing emergence of new opportunities for offending requires a broadening of the parties involved in tackling such problems; hence policy makers and law enforcement must continue to gear up, building relationships with the kind of individuals and organisations recruited for this research so as to remain abreast, if not ahead, of the criminal threats and challenges we will continue to face.

39 Examples include anti-virus software which is often self-updating (assuming an available Internet connection) and the alert and update services available from software providers (though these services normally require the user to proactively check for such information, though a notification service is often available to those who register for it). Third party services such as managed information security providers or free public agencies such as UNIRAS also provide alert services, though again users often have to pre-register.

40 http://www.foresight.gov.uk/.

Technical Appendix A: Criminal threats ranking

Items that are not discussed in the body of the report are shaded.

Threat category	Criminal threat	Threat example	Mean Rating 1=Highly sig. threat, 5=Insig. threat	N=
Paedophilia	Online paedophilia (grooming, possible stalking)	Increased online grooming (possible stalking) using Internet communication mediums (chat, email & messaging platforms).	1.88	26
Espionage	Espionage – Corporate Spies	-	1.89	27
Paedophilia	Online paedophilia (organised crime content selling)	Increased access to purchasers of paedophile content (images, video, sound), sold through the use of various platforms (chat, newsgroups, websites, possibly hosted overseas), sold by organised criminals.	1.89	28
Paedophilia	Online paedophilia (image storage)	Usage of online storage resources (possibly hosted overseas), bypassing seizure of home computers.	1.92	26
Paedophilia	Use of P2P platforms	Use of P2P platforms (distributed and point-to-point) to facilitate & secure online paedophile activity of all types.	1.93	29
Paedophilia	Online paedophilia (secure communications)	Increased secure access to paedophile networks through the use encryption (IP.v6, steganography) & anonymising platforms to bypass policing measures.	1.94	32
Fraud	E-commerce fraud (card not present – PDA/mobile phone devices)	Theft of GPRS PDA/phones (containing personal info & electronic wallets) to achieve online authentication & purchase goods/services.	1.96	25
Paedophilia	Online paedophilia – real time abuse	Increased access by paedophiles to other offenders for the purpose of distributing streamed real time child abuse by criminal paedophiles for personal gratification.	1.96	26
Piracy	Use of P2P platforms	Use of P2P platforms (distributed and point-to-point) to facilitate & secure digital pirate activity of all types.	1.96	26
Paedophilia	Paedophilia (mobile phone grooming)	Increased access to grooming young persons via mobile phones, for the purpose of sexual abuse.	2.00	24
Piracy	IP piracy (warez community exchange)	Increased access to pirate community to trade software & practice, through the use of various platforms (chat/ messaging/ newsgroups/websites – possibly hosted overseas).	2.00	28
Malware	Malicious software (system and organisation impact)	Increasing system impact of malicious software scripts (virus, worm, trojan).	2.00	32
Paedophilia	Online paedophilia (content exchange)	Increased access to paedophile community for the purpose of distributing paedophile content through various platforms (chat/ messaging/ newsgroups/websites, possibly hosted overseas).	2.04	28
Denial of service	BGP DoS malware	Distributed remote denial of service attacks, using various scripts, to flood target systems.	2.04	25
Fraud	E-Govt. fraud (identity theft)	Fraud against online government services (VAT, Income Tax, Tax Credits, DTI licensing) via various techniques (hijacking corporate or individual identities)	2.05	22
CNI/infowar	CNI/Infowar service disruption – data modification	Unauthorised data modification or deletion through unauthorised system access, to disrupt CNI operations.	2.06	18
CNI/infowar	CNI/Infowar (service disruption – DoS attack)	Denial of service using various scripts to flood CNI systems, (CNI attacks sometimes masked by wider DDoS attacks).	2.06	17
Money laundering	Money laundering (overseas online banking)	Money laundering via increased access to overseas 'virtual countries', allowing the bypassing of financial monitoring & other policing measures.	2.06	16
Malware	Malicious software production (password/data grabbers)	Copying and disclosure of authentication details (e.g. passwords) by malicious script.	2.07	30
Hacktivism	Hacktivism (system disruption)	A politically motivated DoS attacks against target organisations systems.	2.07	30

Fraud	General fraud (identity theft involving false document production)	Online data mining (chat rooms, newsgroup, databases, questionable credit reference agencies) to produce false documentation (passport, 'smart' ID cards, medical records) to achieve offline authentication.	2.08	25
Paedophilia	Online paedophilia (third party content storage)	Access to unregulated overseas online storage resources, through the unauthorised use of third party platforms (e.g. corporate or educational networks) bypassing seizure of home computers. Undertaken by criminal IP paedophiles storing content for personal gain.	2.08	25
Malware	Malicious software (mobile device viruses)	Device (e.g. vehicle telematics, digital cameras, PDAs, tablets) data disclosure or corruption.	2.08	24
Paedophilia	Online paedophilia (paedophile community)	Increased access to other paedophiles for sharing of practice & fantasies, using Internet communication mediums (chat/ messaging/ newsgroups/websites, possibly hosted overseas).	2.11	28
Fraud	E-commerce fraud (Identity theft – database hacking)	Unauthorised system access to government & corporate databases, enabling theft of personal information (targeting of individuals of high net worth or specific employees), achieving online authentication for goods/services purchase (particularly financial services).	2.12	26
Denial of service	DNS attack	Attacks on top level domain name servers.	2.15	27
Espionage	Espionage – social engineering	-	2.17	30
Hacktivism	Hacktivism (email service disruption)	A politically motivated denial of email service campaign against target organisation, using information exchange platforms (newsgroup, chat, websites) to encourage & coordinate email flood.	2.17	30
Hacktivism	Online protests (website defacement or hijack)	A politically motivated website defacement or page jacking as part of protest, modifying original website or diverting traffic to alternative website.	2.17	30
Espionage	Espionage – criminal spies	-	2.17	29
Money laundering	Money laundering (overseas online gambling)	Money laundering via increased access to overseas electronic gambling, allowing the bypassing of financial monitoring & other policing measures.	2.18	17
Piracy	IP piracy (warez distribution)	Increased access to distributors of pirate content (software, games, music) through the use of various platforms (chat, newsgroups, websites – possibly hosted overseas).	2.18	28
Malware	Malicious software (mobile phone viruses)	Data disclosure or corruption by mobile phone viruses.	2.22	23
Malware	Malicious software (invisible trojans)	System data disclosure or corruption by invisible trojans. Undertaken by virus writers for CTS.	2.22	27
Espionage	Espionage – spyware	-	2.25	32
Malware	Malicious software (metamorphic viruses)	Unauthorised disclosure, copying, modifying or deleting of data by metamorphic viruses.	2.26	23
CNI/infowar	CNI/Infowar (virus damage)	Unauthorised system data disclosure/corruption or loss of service, by the use of variable payload virus that to copy/modify/delete system data.	2.26	19
Piracy	IP piracy (organised crime content selling)	Increased access to purchasers of pirate content (software, games, music), sold through the use of various platforms (chat, newsgroups, websites – possibly hosted overseas) by organised criminals.	2.28	29
Non-cat.	Black market sales	Increased access to purchasers of unlawful products & services (e.g. unlicensed pharmaceuticals) through various means (websites, newsgroups, chat rooms). Undertaken by unethical companies for commercial advantage (grey market distribution) or criminals for personal gain.	2.28	29
Hardware theft	Hardware theft (portable devices)	Theft of physical hardware -laptops & PDAs- through commercial burglaries and on the street, by criminals for personal gain.	2.29	31
Espionage	Espionage – political spies	-	2.29	24
Fraud	Auction fraud (non-delivered goods)	Fraudulent online auction postings, using social deception techniques, to obtain payment for non-existent items.	2.30	27

Market abuse	Distribution of fake information by various platforms (e.g. newsgroup and bulletin postings, email alerts) to manipulate financial services e.g. share price.	Distribution of fake information by various platforms (e.g. newsgroup and bulletin postings, email alerts) to manipulate financial services e.g. share price.	2.30	20
Denial of service	DRDoS attack	A DoS using a BGP attack virus. These are new protocols currently without authentication.	2.30	20
Fraud	E-commerce fraud (non delivery of goods)	Fraudulent ecommerce, social deception via professional looking website, obtaining payment for non-existent items.	2.30	30
Fraud	Online professional services fraud – investment, banking or other professional services.	Production of content relating to fraudulent investment, banking or other professional service opportunities, achieved by social deception through personalised emails, fake websites, 'investment email' alerts, offshore banks.	2.30	23
Espionage	Espionage – system Penetration	-	2.32	31
Money laundering	Money laundering (online share purchasing)	Money laundering via increased access to online share trading, allowing the bypassing of financial monitoring & other policing measures.	2.33	15
Fraud	E-commerce fraud (stolen credit card details by hacking or intercept)	Unauthorised copying of credit card information, obtained via various means (system penetration, data tap using wireless networks, or a pass-through site), to achieve online authentication & purchase of goods/services.	2.33	30
Non-cat.	Spamming (via third party countries)	The issue of unsolicited emails by mass mailing programs via third party relay countries to avoid anti-spam legislation.	2.34	35
Extortion	Extortion (denial of service – ecommerce)	Threat of denial of service through various means to disable an online e-commerce sites (B2Cor B2B).	2.34	29
Malware	Malicious software (domestic device viruses)	Domestic device (e.g. TV set-top box) data disclosure or corruption.	2.35	23
Market abuse	Fake websites (authenticating fraudulent data) to manipulate financial services e.g. share price.	Fake websites (authenticating fraudulent data) to manipulate financial services e.g. share price.	2.35	20
Denial of service	DoS attack (BGP DoS malware)	DoS attacks using IGMP & RTPs, unauthorised system access and modifying data	2.35	20
CNI/infowar	CNI/Infowar (utility & industrial disruption)	Unauthorised data modification causing system disruption, using various scripts, to Internet & wireless LAN accessible industrial automated control systems (PLC, DCS, SCADA & MMI).	2.35	17
Malware	Trojan mass mailings	Trojan distribution via mass emailings.	2.35	31
Fraud	E-commerce fraud (card not present – data mining source)	Online data mining (chat rooms, newsgroup, databases, questionable credit reference agencies) to achieve fraudulent online authentication (targeting of individuals of high net worth or specific employees) & purchase goods/services.	2.37	27
Non-cat.	Spamming	The issue of unsolicited emails by mass mailing programs.	2.39	33
Espionage	Espionage – device theft	-	2.40	30
Fraud	E-commerce fraud (card not present – offline source)	Fraudulent use of credit card information obtained from offline sources (e.g. receipts) to achieve online authentication & purchase goods (sometimes for re-sale) or services.	2.41	27
Money laundering	Money laundering (online escrow services)	Money laundering via increased access to fraudulent Internet escrow services, allowing the bypassing of financial monitoring & other policing measures.	2.44	16
Fraud	E-commerce fraud (credit card information capture by 'page jacking')	Legitimate website corruption by modifying pages or DNS re-direction, fooling users to enter credit card details to a fake webpage; captured credit card details then used for purchases etc.	2.44	25
Denial of service	GPRS device DoS (mobile phone jamming)	DoS attacks using viral techniques.	2.44	18
Hacktivism	Hacktivism (propaganda – spoof emails)	A politically motivated manipulation of email header information, to send embarrassing emails purporting to be from the target individual or organisation.	2.45	29

Extortion	Extortion (data corruption of automated control systems)	Threat of unauthorised system access to modify data and disrupt Internet and wireless LAN accessible industrial automated control systems (PLC, DCS, SCADA and MMI).	2.45	20
Espionage	Espionage – data tap	-	2.45	31
Non-cat.	Online gambling (risk to underage and vulnerable persons)	Increased access for underage or 'vulnerable' persons to gambling via gambling websites, bypassing physical regulatory measures (e.g. minimum age).	2.46	26
Non-cat.	Fencing (sale of stolen goods)	Increased access to potential purchasers of stolen products through various means (websites, newsgroups, chat rooms).	2.46	28
Espionage	Espionage – employee	-	2.47	30
Non-cat.	Spamming (non SMTP platforms)	The issue of unsolicited emails by non-SMTP platforms (e.g. Instant message, text messages, chat rooms) to avoid anti-spam filters.	2.48	25
Non-cat.	Domestic device disruption (Hacking)	The disruption of domestic digital devices (e.g. set top boxes) to copy or modify data (e.g. access personal account information).	2.48	25
Paedophilia	Online paedophilia – morphed image construction	Production of fake paedophile images using photographic applications.	2.50	26
Piracy	Online piracy (warez storage)	Usage of online storage resources (possibly hosted overseas), bypassing seizure of home computers.	2.50	26
Non-cat.	Online harassment	The stalking of individuals via electronic means (chat rooms, newsgroups, email, website).	2.50	30
Non-cat.	Service theft (wireless bandwidth)	Unauthorised wireless network use via unauthorised system access.	2.50	30
Fraud	E-commerce fraud (goods not fit for purpose)	Fraudulent ecommerce, social deception via professional looking website, obtaining payment for not-fit-for-purpose items.	2.52	27
Fraud	Auction fraud (rigged)	Fraudulent online auction postings using social deception techniques to rig auctions.	2.52	25
Extortion	Extortion (data corruption of business purchasing & distribution systems)	The threat of unauthorised system access to online B2B purchasing portals, to copy/ delete/ modify data and/or deny service.	2.53	19
Espionage	Espionage – hacktivists	-	2.54	28
Extortion	Extortion (data disclosure)	Threat of unauthorised data disclosure through various means (the malicious release of sensitive system data – criminal, medical, financial records).	2.54	26
Extortion	Extortion (malicious data placement)	Threat of unauthorised system access through various means to modify data (the malicious placing of illegal content on a system).	2.54	26
Paedophilia	Online paedophilia – image trading via GPRS mobile phone	Increased access to paedophiles for the purpose of trading of images through the use of GPRS mobile phone platforms.	2.54	26
Non-cat.	Samizdat (misinformation propagation)	Distribution of false/ misleading information through various platforms (chat, websites, newsgroups).	2.56	32
Non-cat.	Hardcore pornography distribution	The publication of pornography that breaches UK law, on websites in unregulated jurisdictions.	2.57	30
Piracy	Satellite service piracy (Software cracks)	Unauthorised access to satellite services by the distribution of software & practice through websites/newsgroups/chat, enabling users to bypass set-top box security measures.	2.60	20
Extortion	Extortion (employee intimidation)	Unauthorised system access through intimidation or blackmail of employees to achieve various data actions.	2.60	25
Fraud	E-commerce fraud (stolen credit card details by keyboard logger)	Unauthorised copying of personal information by a covertly installed key logger application at third party terminals (e.g. cybercafe, library, college), to achieve online authentication & purchase of goods/services.	2.62	26
Fraud	Internal fraud (criminal employees)	Internal fraud (such as procurement or payroll fraud) by unauthorised system access or data disclosure, using various means, by criminal internal employees (or third party insiders) for personal gain.	2.62	26
CNI/infowar	CNI/infowar (service disruption – web defacement)	Unauthorised system access, using various scripts, to deface a web site.	2.63	19
Fraud	E-commerce fraud (credit card number generators)	The production of fake credit card numbers using number card generator programs (e.g. Card Master, Card Wizard) to enable fake transaction authentication.	2.64	25

Piracy	Online piracy (warez storage, unauthorised use of third party resources)	Online storage through unauthorised use of third party platforms (e.g. corporate or educational networks) bypassing seizure of home computers.	2.64	25
Non-cat.	Selling of personal information to spammers	Unauthorised disclosure of personal information (e.g. email address) by the sale of data by one site to another (or a third party). Undertaken by companies or criminal spammers for commercial or personal gain.	2.65	31
Fraud	Fraud (domestic device account access)	The accessing of domestic digital devices (e.g. desktop boxes) through various means to access and copy personal account information by criminals for account hijacking purposes.	2.68	25
Extortion	Extortion (data corruption)	Threat of data corruption through various means.	2.69	26
Fraud	Online 419 fraud	Increased access to potential victims using social deception via fraudulent email, to convince recipients to forward payments.	2.70	30
Fraud	Fraud (online gambling)	Gambling sites obtain bets for rigged gambling.	2.71	21
Piracy	Satellite service piracy (hardware)	Unauthorised access to satellite services by the distribution of hardware & practice through websites/newsgroups/chat, enabling users to bypass desktop box security measures.	2.76	21
Extortion	Extortion (data theft)	Threat of information theft through various means.	2.81	32
Hardware theft	Hardware theft (computers)	Theft of physical system hardware – servers and workstations – through commercial burglaries by criminals for personal gain.	2.90	31
Fraud	E-commerce fraud (credit card reuse)	Fraudulent re-use of credit card details by website owners, after initial legitimate transaction.	2.92	25
Hardware theft	Hardware theft (components)	Theft of system hardware components (chips) in commercial burglaries. Undertaken by criminals for personal gain.	3.06	31
Espionage	Unauthorised disclosure of information through the use of a data tap (particularly wireless networks).		n/a	n/a
Espionage	Unauthorised disclosure of information through unauthorised system access.		n/a	n/a
Espionage	Unauthorised disclosure of information through the use of social engineering.		n/a	n/a
Espionage	Unauthorised disclosure of information through the theft of a device e.g. laptop or PDA.		n/a	n/a
Espionage	Unauthorised system access by use of bespoke spyware or trojan script.		n/a	n/a
Espionage	Unauthorised disclosure of information, by various means, by employees for personal gain or emotional reasons.		n/a	n/a

Technical Appendix B: Technology challenges ranking

Category	Criminal threat	Criminal threat	**Mean Rating** 1=Highly sig. threat, 5=Insig. threat	N=
Email	Online paedophilia (secure communications)	Increased secure access to paedophile networks through the use of encryption (IP.v6, steganography) & anonymising platforms to bypass policing measures.	1.57	21
Non-cat.	Identification systems (including smartcards)	Increasing abuse of immigration processes due to the use and illegal production of 'proof of identity' documents.	1.62	13
Cryptography	Cryptography (secure communications)	Concealment of illegal activities by using *strong cryptography* to establish secure communications (e.g. email).	1.69	26
P2P	Peer-to-peer (covert criminal communications)	Covert means of communication by serious criminals & terrorists.	1.70	20
Non-cat.	Identification systems (including smart cards)	Illegally produced and false documentation used to further illegal activity e.g. fraud.	1.71	14
P2P	Peer-to-peer (offensive content exchange)	Exchange of indecent and offensive material.	1.71	21
Non-cat.	Portals e.g. Yahoo (victim and offender aggregation)	Child pornography exchange and paedophile 'grooming' of children.	1.76	17
P2P	Peer-to-peer platform (distributed)	FreeNet, Morpheus, KazaA, F-Serve.	1.77	22
Websites	Webhosting (criminal exploitation)	Bogus sites, established for fraudulent purposes.	1.79	28
P2P	Peer-to-peer (peer-to-peer networks)	Distribution of copyright material.	1.83	23
P2P	Peer-to-peer platform (system penetration)	Trojan horse functionality in file sharing clients-possible utilisation in DDoS attacks, unauthorised data disclosure.	1.83	18
Non-cat.	Critical national infrastructure IT cabling	Attacks (either physical or logical) on critical points in networks disabling large areas of *telecommunication networks* and corporate systems. Terrorist attacks possibly.	1.83	18
Websites	Webhosting (crime targets)	Targeting of e-services (e.g. e-health, e-govt., e-commerce).	1.85	26
Cryptography	Cryptography (secure storage)	Concealment of illegal activities via using *strong cryptography* to establish secure storage.	1.85	26
Non-cat.	Portable high-capacity storage devices	Ease of use and transport. Low risk of detection.	1.86	21
Non-cat.	Critical national infrastructure IT power supplies	Attacks (either physical or Hi-tech) on critical points in *power supplies* disabling large areas of society and affecting systems.	1.87	15
Broadband	Broadband services (unauthorized data disclosure – personal data for Identify theft)	Identity theft following a hacking attack to allow access to illegal material anonymously.	1.88	24
Non-cat.	Forensic evidence eliminators	Cleaning out PCs of incriminating materials e.g. paedophiles.	1.88	24
Mobile communications	Mobile communications (NG)	User anonymity for criminals & terrorists.	1.88	25
Non-cat.	Encryption (privacy technique)	Increased use of encryption for Internet transactions and PC file protection.	1.91	23
Cryptography	Stenography (secure communications)	Concealment of criminal activities via *stenography* to enable secure communications.	1.92	24
Websites	Webhosting (unregulated overseas)	Offshore hosting.	1.93	27

Websites	Use of P2P platforms	Use of P2P platforms (distributed and point-to-point) to facilitate & secure online paedophile activity of all types.	1.94	18
Cryptography	Encrypted processing	On the fly encryption of all PC processes, data and applications.	1.95	19
Broadband	Broadband service (facilitate P2P networks)	Faster, always on nodes will increase use of peer-to-peer links.	1.95	22
Non-cat.	Chat platforms e.g. IRC, IM (distribution medium for illegal or mischievous content)	Distribution of illegal material e.g. paedophiles, IP pirates.	1.96	25
Wireless networks	Wireless networks (service theft)	Theft of service (bandwidth) by tapping into wireless network & using for transmitting data.	2.00	17
Non-cat.	Digital cameras	Paedophile use for targeting the young.	2.00	18
Non-cat.	Tools availability of attack tools on the Internet	Attackers with limited IT skills can use the available tools for a wide range of attacks. These tools will lead to increased numbers of virus in the wild and sniffing attacks and system penetrations.	2.00	21
Non-cat.	Children's access to the Internet at home and school	Vulnerability to paedophiles.	2.00	21
Broadband	Broadband services (service theft)	Attacks on insecure home machines giving intruders control of very large bandwidth and CPU resources for large-scale attacks.	2.00	26
Anonymisation	Anonymity (lack of access authentication)	Ability to 'safely' send illegal communications (content or intent) due to lack of authentication required for Internet café or kiosk service.	2.04	26
Websites	Webhosting (crime enabler)	Collection of information for social engineering purposes.	2.04	25
Anonymisation	Anonymisation	Attacks relayed through third party hosts.	2.04	23
Non-cat.	High quality digital recording equipment	Pirate films being made available on the Internet for either purchase or for free.	2.05	21
Non-cat.	Digital content (piracy)	IP infringement – unauthorised imitation of data related products.	2.05	20
Wireless networks	Wireless networks (mobile offenders)	Wireless transmission of real time paedophile abuse.	2.06	16
Non-cat.	Electronic cash	Money laundering potential.	2.06	16
Non-cat.	Internet technologies	In addition to attack on web-connected systems, expect indirect attacks against back end systems (.e.g. database servers) to which they are connected.	2.06	16
Mobile communications	Misuse of Pay As You Go mobile, 3G and/or WAP technology	E-theft.	2.07	15
Non-cat.	Online gambling	Passing money using conventional credit cards provides a means to export large sums in an unregulated environment.	2.07	15
Non-cat.	Gaming sites	Money laundering – opportunity to use an apparently bona fide operation as a front for sourcing incomes.	2.07	14
Non-cat.	Public Internet access points (cafes, kiosks, hotels)	Enables anonymous access to Internet by criminals and terrorists.	2.08	25
Non-cat.	Voice over IP (VoIP)	Enabling of global networking & expansion of criminal enterprises with encrypted voice communications.	2.08	12
Broadband	Broadband service and compression (facilitate illicit data transfer – remote storage)	Facilitate remote storage of illicit material.	2.08	24
Mobile communications	Mobile photo phones (image distribution)	Distribution of pornography.	2.10	21
Cryptography	Private key theft	Theft or compromise of private keys	2.10	21
Non-cat.	Payment system ENV technology	Exploit authentication/ encryption weaknesses.	2.10	10
P2P	Peer-to-peer (secure data distribution & storage)	Use of distributed & encrypted P2P platforms to anonymously share data.	2.10	20
Non-cat.	Children's access to the Internet at home and the school.	Vulnerability to other forms of abuse – bullying, malicious threats etc.	2.10	20

Mobile communications	Misuse of Pay As You Go mobile, 3G and/or WAP technology	Fraud.	2.12	17
Non-cat.	Online finance systems	Interference with regulatory and financial software.	2.12	17
Non-cat.	Spoofing domains	Spoofing domains by attacks on DNS servers.	2.12	17
Anonymisation	Anonymisation (open mail relay & anonymisation services)	Ability to 'safely' send illegal communications (content or intent).	2.12	25
Wireless networks	Wireless networks (service theft for next hop)	Remote activation of material therefore unable to source originator.	2.13	16
Non-cat.	Laptop and palmtop computer technology	System penetration by mobile offenders.	2.14	22
Non-cat.	Smart card applications (data modification)	Falsifying data to undertake fraud (i.e. increasing monetary values, identity theft)	2.15	13
Email	Email (distribution cut-out)	Email addresses taken out with bogus user registration details	2.15	26
Non-cat.	Online storage, i.e. data held within another jurisdiction	Safe 'dead drop' storage of illicit data e.g. espionage or crime.	2.16	19
Anonymisation	Anonymity (lack of mail authentication)	Ability to 'safely' send illegal communications helped by lack of authentication for mail account registration.	2.16	25
Websites	Webhosting (crime enabler)	Websites containing information that facilitates the perpetration of crimes (e.g. hacker sites, with advice and tools).	2.19	27
Non-cat.	Electronic cash	Cyber-laundering.	2.19	16
Mobile communications	Mobile phones/PDAs	Targets for theft.	2.19	21
Mobile communications	Mobile photo phones (espionage)	Espionage.	2.22	18
Non-cat.	Chat platforms (communication medium for illegal activity)	Covert means of communication by criminals and terrorists.	2.23	22
Non-cat.	Credit and ATM cards	Abuse of ATM systems and EPOS procedures.	2.25	16
Email	Email (spam)	The sending of unsolicited email, causing network and storage congestion.	2.26	27
Non-cat.	Domain name service (hijack)	Alteration of information by unauthorised persons.	2.27	15
Non-cat.	IP telephony (anonymous voice communications)	The use of IP telephones to conduct voice calls over the Internet, with anonymity and encryption.	2.27	15
Non-cat.	Remote system upgrades/monitoring and fault diagnosis.	Adoption as a network link to end systems by attackers.	2.27	15
Non-cat.	Online gambling	Provides a means to empty accounts of stolen credit cards that is totally deniable by the receiver.	2.29	14
Non-cat.	Data volume	Volume of data that is stored and processed. Criminals will rely on the fact that the more data and transactions there are, the less likely they are to be caught	2.30	20
Mobile communications	Mobile phones (service theft – chipping)	Illegal reprogramming of chips/SIM cards/IMEI numbers – allowing 'free' illegal use of phones.	2.31	16
Non-cat.	Online auctions (Trading Standards)	Item sold is not item advertised.	2.32	19
Websites	Website hacktivism (site defacements)	Hacktivism – An individual or group is trying to make a public statement by defacing the companies website.	2.32	22
Non-cat.	Gaming sites	Fraud.	2.33	12
Non-cat.	Complexity	Criminals will use the complexity of systems to hide or disguise their activity.	2.33	21
Non-cat.	Public Internet access points (cafes, kiosks, hotels)	Interception of communications by bugging public access points.	2.33	21
Email	Email (distribution medium for harmful content – malicious software)	Trojan.	2.33	24
Email	Email (distribution medium for harmful content – fraudulent)	Distribution via spammed mailings of fake investment offers etc.	2.33	24
P2P	Peer-to-peer platform (IM)	IM (Instant messaging software)	2.35	23

Non-cat.	Reverse engineering	Criminals nowadays often employ reverse engineering techniques to ascertain how a device is manufactured, in order to produce counterfeit version.	2.35	20
Non-cat.	Trojanised digital content	Trojans and virus added to pirated software applications.	2.35	17
Websites	Webhosting (media platform)	Propaganda outlet for undesirable activities.	2.37	27
Broadband	Broadband services (service theft – storage)	Theft of disk space following an attack to store illegal material on a home computer without detection.	2.38	26
Mobile communications	Mobile photo phones (facilitate criminal orchestration)	Data and imaging capability of mobile phones used to organise and manage riots.	2.39	18
Non-cat.	Network sniffers (information disclosure by data tap)	Sniffers used to read unencrypted data flowing across networks, providing unauthorised access to confidential information (e.g. passwords).	2.39	18
Non-cat.	Internet-aware appliances (home, car, etc.)	Malign parties joining self-organising broadcast networks (e.g. Bluetooth).	2.40	10
Mobile communications	Mobile phone/GPS devices	Paedophiles would find the locating device on mobiles useful.	2.40	15
Non-cat.	Digital cameras	Invasion of privacy by unauthorised remote activation.	2.41	17
Non-cat.	Forensic evidence eliminators	New anonymising services from service providers.	2.41	17
Non-cat.	Online directories and open source information	The problem is already here and is open to exploit and abuse.	2.41	17
Mobile communications	Mobile communications (service theft – network hack)	Fraudulent access to services.	2.42	12
Non-cat.	Biometric applications (data corruption)	Alter or delete data to compromise correct identification.	2.42	12
Websites	Online paedophilia – morphed image construction	Production of fake paedophile images using photographic applications.	2.42	19
Non-cat.	Games consoles	Games consoles allowing storage as well as interoperability. Mod chips allowing greater opportunity for misuse.	2.43	14
Broadband	Broadband services (secretion of illicit material)	Insertion of illegal material on a home or work computer to cause reputational damage.	2.43	23
Email	Email (distribution medium for harmful content – malicious software)	Distribution of blended threat viruses.	2.43	23
Wireless networks	Wireless/ Bluetooth (home network disruption)	Nuisance attacks against household systems by penetrating home-based wireless networked system.	2.44	18
P2P	Peer-to-peer platform (IRC)	IRC (Internet relay chat).	2.45	22
Email	Email (distribution medium for offensive content – pornography)	Pornography.	2.46	24
Wireless networks	Wireless networks (DoS attack)	System DDoS attacks via wireless transmission.	2.47	15
Non-cat.	IP routers and telecommunications switches	Denial of service, masquerade attacks and control of/free use of communications infrastructures.	2.47	15
Non-cat.	Network scanner (system penetration)	Scanners used to find weak links in firewalls and network configuration.	2.47	19
Non-cat.	Intrusion testing tools	System penetration.	2.48	21
Non-cat.	Biometrics (system penetration)	Accessing the digital code created by the biometric reader, or held in the reference database, and injecting this into a system behind the reader, to gain access.	2.50	12
Non-cat.	Internet-aware appliances (home, car, etc.)	Compromise of electronic system with large potential real-world impact.	2.50	14
Non-cat.	Chat platforms (medium for online harassment)	Harassment via chat rooms (IRC) or instant messaging services (AOL Instant Messaging).	2.50	18
Email	Email analysis software (malicious privacy breach)	Unauthorised monitoring of email for personal motives, potential for blackmail.	2.50	22

Non-cat.	Drive to bring products to market in minimal lead times leaves security provisions low down in developments priorities.	Across the board, criminals have minimal software security measures to overcome.	2.50	22
Websites	Webhosting (crime communities)	Scorekeeping – groups or individuals trying to rack up the most number of defaced sites. For them, this is mainly an intellectual pursuit for bragging rights.	2.53	19
Mobile communications	Mobile communications (data tap)	Intercepting communications.	2.54	13
Non-cat.	Neural networks and data mining techniques of open online information sources	System penetration with acquired public information.	2.54	13
Non-cat.	Internet routing protocols, BGP in particular	Denial of service attacks and possibly a BGP worm.	2.55	11
Non-cat.	Forensic evidence eliminators	Removal of routing information from network records.	2.55	20
Non-cat.	Biometric applications (data corruption)	Implant data to generate false identities.	2.57	14
Non-cat.	Remote access	Use of remote access by employees or partners.	2.57	21
Non-cat.	FTP (distribution of illegal material)	Distribution of indecent or copyrighted material.	2.59	22
Non-cat.	Real-Time Transport Protocol	Session hijacking for protocols such as voice over IP (which uses RTP)	2.63	8
Mobile communications	Mobile communications (DoS)	DDoS via SMS.	2.64	11
Non-cat.	FTP (covert communications)	Covert means of communication by serious criminals or terrorists.	2.64	14
Non-cat.	Digital piracy (wireless distribution)	Distributed pirate content services.	2.65	17
Non-cat.	Digital CCTV systems	Alteration or denial of service attacks rendering surveillance systems inoperable.	2.67	12
Non-cat.	Microsoft operating systems	Shatter attacks.	2.67	18
Non-cat.	The current Internet Protocol (v5) can be spoofed.	Masquerading as another, fraudulent authentication.	2.69	16
Non-cat.	Drive to bring products to market in minimal lead times leaves security provisions low down in developments priorities.	Insiders' in software companies can insert malicious code for future criminal exploitation with little fear of discovery.	2.70	20
Non-cat.	Domain name service	Registration of 'misprints' close to well-known sites.	2.71	17
Email	Email analysis software (privacy breach)	Monitoring of email for work purposes.	2.76	21
Websites	Webhosting (media platform)	Rival company sponsored PR campaign.	2.80	15
Non-cat.	Security alerts and advisory services	Bogus security advisories and alerts, exploiting published vulnerabilities.	2.80	20
P2P	Peer-to-peer platform (FTP)	FTP (File Transfer Protocol).	2.90	21
Wireless networks	Wireless networks (service theft for next hop)	Obtain anonymity through other systems. Relay points for further attacks.	2.94	17
Wireless networks	Wireless networks (system penetration)	Unauthorised penetration of network from a nearby listening site.	2.95	19
Broadband	Broadband services (data theft or copying)	Hacking attacks on home computers to 'steal' music or movie files.	3.13	24
Wireless Networks	Wireless networks (network data tap)	Unauthorised interception of network traffic.	3.17	18
Mobile communications	Mobile communications (DoS)	Jamming, denying communications.	3.18	11
Non-cat.	Video conferencing (medium for online harassment)	Harassment via video conferencing.	3.22	9

Appendix C: Acknowledged panel participants

The following participants completed all rounds of the survey and agreed to be cited, whilst a number of additional participants declined to be acknowledged. Thanks goes also to other participants who completed a number, but not all rounds of the survey.

J Ames, Home Office

Peter Anaman, Business Software Alliance

Dr. Andrew Blyth, University of Glamorgan

Paul Brennan, Federation Against Software Theft

Bruno Brunskill, Anite Public Sector

Martin Carden, NTL

John Carr, NCH

Richard Clayton, University of Cambridge

Andrew Cormack, UKERNA

Geoff Fellows, Northamptonshire Police

Dr. Steve Furnell, University of Plymouth

Riten Gohil, APACS

Mike Haley, Office of Fair Trading

Clive Hawkswood, Department for Culture, Media and Sport

Ian Hodges, HM Customs & Excise

Simon Janes, Ibas Computer Forensics

Tony Lever, BT

John MacGowan, Consultant

Dr Allyson MacVean, Buckinghamshire Chilterns University College

Dr. Frank Marsh, British American Tobacco plc

Vijay Mistry, National Hi-Tech Crime Unit

Michael A. Penhallurick, South Yorkshire Police

Steven Philippsohn, Philippsohn Crawfords Berwald

Andrew Powell, National Infrastructure Security Co-ordination Centre

Peter Robbins QPM, Internet Watch Foundation

Dr L.W. Russell, Forensic Science Service

Peter Sommer, London School of Economics

Richard Starnes, Cable and Wireless

Professor Michael Walker, Vodafone Group Services & Royal Holloway, University of London

Graham Walsh, Federation Against Copyright Theft Ltd

Jeff Yan, University of Cambridge

Peter Yapp, Control Risks Group

References

@stake (2003) Security advisory issued 25 February 2003 (http://www.@stake.com/research/advisories/2003/a022503-1.txt).

ARC Group (2003) *Future Mobile Computing* briefing (http://www.the-arc-group.com/).

ARC Group (2002) *Mobile Payments* briefing (http://www.the-arc-group.com/).

BusinessWeek Online (2003) Online article *Cyber-Extortion: When Data is Held Hostage* (http://www.businessweek.com/bwdaily/dnflash/aug2000/nf20000822_308.htm).

Carr, J. (2004) *Child abuse, child pornography and the Internet* The National Children's Homes.

Casey, E. (2000) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* Academic Press.

Clarke, N.L., Furnell. S. M., Rodwell, P. M. and Reynolds, P. L. (2002) Acceptance of Subscriber Authentication Methods for Mobile Telephony Devices, *Computers and Security*, Volume 21, Number 3.

Computers and Security (2002:1) *Wireless Network Security Concerns*, Volume 21, No. 1, 11.

Computers and Security (2002:2) *Wireless Networking Compromises Customer Credit Card Numbers*, Volume 21, No. 4.

ComputerWeekly.com (2003:1) Online article *Gartner security conference: Worry more about insiders than cyberterrorists* (http://www.computerweekly.com/articles/article.asp?liArticleID=122331).

ComputerWeekly.com (2003:2) Online article, *Nuclear energy firm slashes its costs by switching to Blackberry* (http://www.computerweekly.co.uk/articles/article.asp?liArticleID=122634&liArticleTypeID=1&liCategoryID=1&liChannelID=2&liFlavourID=1&sSearch=&nPage=1).

Coutorie, L. E. (1995) The Future of High Technology Crime: A Parallel Delphi Study *Journal of Criminal Justice*, Vol. 23, No. 1, pp.13-27.

Ekblom, P. (1997) Gearing up against crime: a dynamic framework to help designers keep with the adaptive criminal in a changing world *International Journal of Risk, Security and Crime Prevention*, October 1997, Vol.2/4: 249-265.

Financial Action Task Force on Money Laundering (2003) *The Forty Recommendations.* (http://www1.oecd.org/fatf/).

Financial Action Task Force on Money Laundering (2003) *Report on Money Laundering Typologies 2002-2003*. (http://www1.oecd.org/fatf/).

Financial Action Task Force on Money Laundering (2000) *Report on Money Laundering Typologies 1999 - 2000* (http://www1.oecd.org/fatf/)

Financial Action Task Force on Money Laundering (1998) *1997 – 1998 Report on Money Laundering Typologies 2002-2003* (http://www1.oecd.org/fatf/).

GAO (2003) File Sharing Programs: Child Pornography is Readily Accessible over Peer-to-Peer Networks Government *Accounting Testimony* (www.gao.gov/new.items/d03537t.pdf).

Guardian (2000) Online article, *Pump and dump' boy is unrepentant* (http://www.guardian.co.uk/Print/0,3858,4080201,00.html).

Guardian Online (2003) Online article, *Mobile phone ban amid child sex fears: Council halts picture messaging in leisure centre* (http://www.guardian.co.uk/uk_news/story/0,3604,960427,00.html).

Human Firewall (2002) Online article *Workers give Passwords to Total Strangers in Scruples Survey* (http://www.humanfirewall.org/scruples.htm).

Information Management & Computer Security (1995) *Hackers threaten medical security*, Volume 5, Number 4, 157.

Information Management & Computer Security (1999:1) *US key target of corporate spies*, Volume 7, Number 2, 103.

Information Management & Computer Security (1999: 2) *Investors caught in Net scam*, Volume 7, Number 3, 160.

Information Management & Computer Security (2000) *Viruses could wipe nation off Internet map*, Volume 8, Number 5, 250.

Information Management & Computer Security (2001:1) *Hackers targeting big firms*, Volume 9, Number 1, 52.

Information Management & Computer Security (2001:2) *Arab hackers hit Israeli sites*, Volume 9, Number 1, 54.

Information Management & Computer Security (2001:3) *Wireless devices next target for viruses: McAfee*, Volume 9, Number 2, 102.

Information Management & Computer Security (2001:4) *Mobile Computer Systems – security considerations*, Volume 9, Number 3, 134-136.

ISRM (2003) *Photography of children in sport and recreation centres* Institute of Sport and Recreation Management Information Note (http://www.isrm.co.uk/news/photo.htm).

Hyde-Bales, K., Morris, S. and Charlton, A. (2004) *The Policing Recording of Computer Crime* Development and Practitioner Report 40/04, London: Home Office.

Lang, T. (1995) An Overview of Four Futures Methodologies *Manoa Journal of Fried and Half-Fried Ideas*, Volume Seven: Occasional Paper Seven – August, Hawaii Research Center for Future Studies.

McVean, A and Spindler, P. (2003) *Policing Paedophiles on the Internet* The John Grieve Centre for Policing and Community Safety.

Mann and Sutton (1998) NetCrime: More Change in the Organisation of Thieving *British Journal of Criminology*, Vol.38, No.2. Spring.

MessageLabs (2002) Online December 2002 press briefing available at http://www.messagelabs.com/news/pressreleases/detail/default.asp?contentItemId=118&region=.

Morris, S. (2004) *The future of netcrime now: Part 2 – responses* Online Report, London: Home Office.

NCSA (2003) *Fast and Present Danger* A National Cyber Security Alliance survey (http://www.staysafeonline.info/).

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

Oftel (2003) *Oftel's Internet and Broadband Brief – 10/12/ 2003.* (http://www.ofcom.org.uk/research/consumer_audience_research/telecoms/wireless_update/wirelessbroadband/.

PointSec (2003) Online article, *Survey Reveals Stolen PDAs Provide Open Door To Corporate Networks* (http://www.pointsec.com/news/news_pressrelease_aug13-03-UK.asp).

Power, R. (2000) *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace*, QUE Corporation: Indiana.

Preble J (1983). Public Sector Use of the Delphi Technique in *Technological Forecasting and Social Change* Vol 23, pp 75-88.

Silicon.com (2003:1) Online article *Barclays is latest target of spoofed website fraud*. (http://silicon.com/news/500019-500022/1/6005.html).

Silicon.com (2003:2) Online article, *Camera phones set to rocket*. (http://www.silicon.com/news/500018/14/5653.html .

Silicon.com (2003:3) Online article, *IT firms shout out spying cameras*. (http://www.silicon.com/news/500018/1/5031.html).

Silicon.com (2003:4) Online article, *Corporates get serious with texting*. (http://www.silicon.com/news/164/1/5125.html).

Sunday Mail (2003) Online article, *Paedophiles Hijack Becks Phone Cams*. (http://www.sundaymail.co.uk/news/page.cfm?objectid=12894468&method=full&siteid=86024&headline=PAEDOPHILES%20HIJACK%20BECKS%20PHONE%20CAMS).

Symantec (2003) Online article, *Fake Bank Web Site Scam Reaches U.S*. (http://enterprisesecurity.symantec.com/content.cfm?articleID=2205&PID=16515047&EID=401).

Symantec, 2003:2 Symantec Security response briefing *W32.Mant.Worm*. (http://securityresponse.symantec.com/avcenter/venc/data/w32.mant.worm.html).

Tafoya, W.L. (1986) *A Delphi forecast of the future of law enforcement* Unpublished doctoral dissertation, The University of Maryland.

VNUNET (2000) Online article, *More big Net names fall victim to vandalism* (http://www.vnunet.com/News/106320).

ZDNet (2002) Online article, Government *urged to act on wireless broadband*. (http://news.zdnet.co.uk/Internet/0,39020369,2126495,00.htm).

ZDNet (2003:1) Online article, *Trojan horse found responsible for child porn* 1 August 2003. (http://news.zdnet.co.uk/Internet/security/0,39020375,39115422,00.htm).

ZDNet (2003:2) Online article, '*Wi-Fi anonymity tempts pirates* 16 July 2003. (http://news.zdnet.co.uk/Internet/0,39020369,2137649,00.htm).

Woudenberg, F. (1991) An Evaluation of Delphi *Technological Forecasting and Social Change 40*, 131-150.

Produced by the Research Development and Statistics Directorate, Home Office

This document is available only in Adobe Portable Document Format (**PDF**) through the RDS website

Home Office
Research, Development and Statistics Directorate
Communication Development Unit
Email: publications.rds@homeoffice.gsi.gov.uk

ISBN 1 84473 498 6