Oxford Internet Institute, Forum Discussion Paper No. 6, November 2005

Rethinking safety and security in a networked world: reducing harm by increasing cooperation

Victoria Nash

Oxford Internet Institute
University of Oxford
1 St Giles, OX1 3JS
Oxford, UK

Malcolm Peltu

Oxford Internet Institute,
University of Oxford
1 St Giles, OX1 3JS
Oxford, UK

Foreword

Against the backdrop of increasing and often sensational media coverage about the potential abuse of the Internet by spammers, hackers, paedophiles and terrorists, the Oxford Internet Institute (OII) and a number of partners organised a conference on 8–10 September 2005 that sought to examine whether, and how, such fears are changing the complex and delicate balance of values and interests at stake in the Internet's global network of networks. Called *Safety and Security in a Networked World: Balancing Cyber-rights and Responsibilities*, the conference focused on two aspects associated with risks arising from the use of the Internet and related information and communication technologies (ICTs): personal safety online, and the security of the networks and systems being used.

These safety and security dimensions receive much political and media attention, but are rarely considered together. The Conference Organising Committee therefore sought to encourage a productive dialogue between experts from both these communities and other relevant stakeholders. The aim was to better inform agendas for international government–industry cooperation at all levels by enhancing understanding of the key problems and possible responses in these areas.

Over 140 people attended the event, and forty-one papers were chosen for presentation at the conference out of more than 70 abstracts submitted. Participants included representatives from non-governmental organisations (NGOs), mainly concerned with child safety, government policy makers, law enforcement officials, regulators, ICT suppliers, researchers, educationalists, and technical experts.

This discussion paper draws primarily on presentations, papers and discussions at the event in summarising the main themes and findings that emerged from the conference. Further background, including papers, webcasts of key sessions and interviews with some participants, is available on the OII website (www.oii.ox.ac.uk/research/cybersafety).

The conference was sponsored by, and organised in cooperation with, the University of Auckland, NetSafe, EURIM and the Watson Institute for International Studies at Brown University.

Dr Victoria Nash
OII Policy and Research Officer
Conference Organising Committee Chair

Acknowledgements

As Chair of the Conference Organising Committee, I am indebted to the immense contribution to the planning and running of the event made by my colleagues on the Committee: Liz Butterfield, Director, NetSafe; John Carr, International Internet Consultant on Child Safety; Professor James der Derian, Director, Watson Institute for International Studies, Brown University; Professor John Hosking, Head of Computing Department, University of Auckland; Professor Gloria Laycock, Director, Jill Dando Institute of Crime Science; and Philip Virgo, Secretary General, EURIM.

In-kind support from the University of Auckland, NetSafe, EURIM and the Watson Institute was much appreciated and we are also very grateful to Nominet for sponsoring the conference reception. We were also greatly assisted by being able to build on the experience gained by NetSafe (an Internet Safety Group backed by the New Zealand government) and the University of Auckland in organising previous events on online safety in the home, workplace, business and schools.

As co-author of this report, I would also like to thank all participants in the event: speakers, delegates, session chairs and rapporteurs. Their talks, papers and lively and questioning contributions to discussions provided a rich source, even where specific individuals could not be credited. The authors take sole responsibility for the interpretation of this material.

Special credit for the smooth and efficient running of the event is due to all the OII support staff who helped organise this conference, especially Lucy Martin, Suzanne Henry, Adham Tamer, Arthur Bullard, David Sutcliffe, Kunika Kono and Tom King.

Victoria Nash
OII Policy and Research Officer
Conference Organising Committee Chair

Executive summary

The OII Conference was organised to facilitate dialogue between citizens, users, governments, law enforcement agencies, industry and education on issues of personal Internet safety and the security of networks and systems. Its primary aim was thus to help inform decision-making by supporting a more sophisticated understanding of both the problems surrounding Internet safety and security and the possible responses.

The following points summarise some of the key findings to emerge from the conference in relation to this aim:

Understanding the nature of the problem

- We need to broaden the focus of Internet safety concerns, recognising that, as well as children, some teenagers and adults may be 'vulnerable' users of the Internet and also that different types of content may be harmful for different users. Adopting such a perspective in both research and policy should enable us to better protect or help those who need it most.
- It is simply not helpful to treat activity or experiences in the 'offline' world as separate from those in the 'online' world as there is rarely such a clear demarcation in practice.
- Quick and easy 'solutions' to the problems highlighted will be hard to find, as there are many conflicting values and interests involved. It should also be recognised that most ICTs are 'double-edged', in that the same capability can be used for socially beneficial and destructive ends—so policy options such as banning or restricting access to certain types of ICT will always involve trade-offs.
- Outcomes from decisions and policies relating to online safety and security are unpredictable because they arise from complex interactions between multiple actors with differing goals across many sectors or jurisdictions.
- More research is needed to inform judgments in policy making, particularly social research that gathers better empirical evidence of the specific perceptions, habits and needs of particular users and consumers of the Internet and related ICTs, and of the social and institutional contexts of their use.
- The 'politics of language' can hinder clear understanding of Internet safety and security issues as terms such as privacy or pornography have different emotional and conceptual implications for different people in different contexts.

Possible responses

- Positive developments in policy and practice could be gained if the traditionally very separate personal safety and cyber-security communities could learn to collaborate more.
- Slow pragmatism pays off: exploring local and international collaboration on a case-by-case basis and building on existing partnerships offers potentially the most fruitful way forward.
- There is no need to start from scratch: because online and 'real-world' issues are intertwined, existing policy options can often be adapted to meet the new policy challenges thrown up by the Internet. In addition, long-gathered experience and expertise should be employed to enhance implementation of new policies.
- Although regulatory and technical measures are often sought to reduce online risks, more imaginative and extensive use should be made of a wide range of social, economic and institutional levers, such as education, financial incentives, job training or even attempts to encourage more responsible media coverage.
- Where policy and regulatory processes are employed, they must be flexible enough to keep pace with rapid innovation in ICTs. Such policies will be most effective if accompanied by efforts to overcome institutional inertia to ensure that change is not resisted.
- In order to ensure that safety and security concerns do not undermine growth in Internet use and potential, it is necessary to consider all available policy options, including the ideologically taboo issue of restricting the Internet's openness, such as through more intervention by the Internet's central infrastructure.
- Insight gained in disciplines focusing on the management, assessment, perception and communication of risk could be of great value in helping to place online risks and benefits in a balanced context, with a focus on practical harm reduction rather than demands for quick solutions and hysterical over-reaction that often dominate public discourse in this field.
- Finally, progress is possible: the conference highlighted many examples of promising local, national and international regulatory, legal, inter-agency and multi-stakeholder initiatives, despite concerns that differences of law, politics and culture would make cooperation on these issues extremely difficult.

Outline of this paper

This paper reports on the themes emerging from the conference in relation to the prime aims of the event. The Introduction explains the value of connecting debates around safety and security aspects of ICT networks, and highlights the challenges which are raised by the contexts in which networked technologies are used. Section II seeks to clarify the nature of the safety and security issues and problems raised, including value conflicts and other disagreements that need to be accommodated and balanced. Possible responses which might achieve workable resolutions to online safety and security concerns are summarised in Section III, taking account of legal, national, social, institutional and cultural differences and the impacts of rapid innovation in ICTs and their application. The conclusion identifies future opportunities and challenges in addressing Internet safety and security issues. Specialists terms used in this paper are explained in the Glossary at the end.

I Introduction

Why safety and security?

‘Safety’ and ‘security’ are closely matched synonyms, often used interchangeably in conversation. Why then have a conference which explicitly aims to explore issues around both safety and security? An answer lies in one of three themes that ran through the event: the importance of the ‘politics of language’, where even the apparently simplest words are often charged with deeper, often conflicting, values, meanings and cultural and institutional associations.

The term ‘safety’ in relation to the Internet and related ICTs has become associated with the activities of NGOs, government agencies, experts, local groups and other stakeholders whose policy agendas prioritise issues of personal safety and harm in online worlds, particularly those concerning children. An equivalent ‘cybersecurity’ community has evolved over a longer period of ICT development, anchored in more technical, institutional, economic and regulatory concerns, such as safeguarding network, business and government infrastructures. In short, the safety of people is the prime concern of one group and the security of ICT systems of the other.

Of course, these personal safety and network security communities overlap considerably, for example in their mutual interest in questions of protection against criminal acts or unwarranted access to confidential data, and each is far more nuanced than indicated by these broad descriptions. However, discussions and analyses at the conference clearly demonstrated distinctive cultures and agendas associated with each perspective. Their concerns are frequently covered together as part of campaigns to support improved media literacy and computer skills, but much less so in policy and research activities.

The synergy at the conference that resulted from its intensive coverage of both areas, as described in this report, shows that continuing dialogue and sharing of knowledge can be a significant step towards finding appropriate responses that address both the numerous problems identified and help to realise the enormous potential benefits of a more networked world. Table 1 summarises a small selection of the vast number of relevant issues raised, as explored in the remainder of this paper.

The challenges of context

In addition to specific security- or safety-related concerns, some discussion focused on challenges posed by the practical and normative contexts in which networked technologies are used. The rate of technological advance poses decision and policy-makers with a great challenge, providing new means of resolving problems at the same rate as new concerns arise. The Internet does not naturally respect national boundaries, so addressing security or safety risks will often involve require a degree of international cooperation. Achieving such cooperation is made all the more difficult by the fact that issues of security or safety are themselves understood against a backdrop of broader social, cultural and political values which may vary across nations or regions.

Table 1. Examples of safety and security issues addressed at the conference

Safety	Protection of children using the Internet and mobile cellphones
	Family/school/community responsibilities in educating children about online risk
	Paedophile contact via online chat rooms
	Cyber-bullying via mobile phones and the Internet
	‘Digital dossiers’ recording details of an individual’s life
	Addiction by adults and children to online games
	Suicide and self-harm websites
Security	Personal security (e.g. theft of personal information such as banking details)
	Computer security (e.g. viruses and unwanted spam emails)
	Network security (e.g. ‘hacking’ to break network security or denial-of-service attacks on websites)
	National security (e.g. terrorism)
	Digital identification and authorisation
	Tracking network traffic across borders and jurisdictions
	Data protection
	Intellectual Property Right (IPR) protection on digital media

It is perhaps informative, that even at this high-level conference, some of the most vigorous debates arose from disagreement about these underlying values. For instance, discussion of steps towards greater international cooperation in the fight against child pornography generated a heated debate about the First Amendment to the US Constitution which protects the right of free speech including through digital media. Some speakers argued this has created difficulties in prosecuting and closing down the many US-based websites hosting child pornography content, as they could be seen to be protected unless it is proven that they are images of actual children engaged in the illegal acts depicted. Others emphasised that the Amendment guaranteed a fundamental human right, and that further, it did not hinder prosecution.

This discussion revealed how bringing together Internet-interested safety and security communities can be of value in highlighting the cultural and other contexts that make dealing with such policy issues particularly challenging. It also highlights the key role played by conflicts that derive from differences in values, perceptions and legal and national differences. This indicates why many ‘technical fixes’ or regulatory action can, at best, be only a partial or temporary resolution of the problem addressed. At the same time, addressing more technically oriented problems and uncertainties created by rapid and interlinked innovations in converging networked digital technologies should also be prioritised, to ensure the speed of response keeps pace with technical change. What is said to be technically or economically impractical or even impossible now may become commonplace soon.

Addressing effectively the kinds of issues illustrated in Table 1 therefore requires close and ongoing collaboration between local, national and international stakeholders, including NGOs, government agencies, regulators, business professionals, ICT experts, researchers and the wider community.

II Clarifying cyber-safety and security issues

Defining the problems

Clarifying the nature of both safety and security problems related to ICT networks and their interaction was a central theme of discussions at the conference. This was deemed to be a valuable contribution to the policy debate in so far as a more nuanced understanding of such problems should support more effective decision-making at all levels. With this aim in mind, one of the conference’s clearest messages was the need to broaden the scope of the personal cyber-safety agenda so that it could address concerns relating to all vulnerable users and types of material, not just the risks to children of paedophile contact and access to adult material that have been the headline concern of most Internet safety campaigns.

For instance, many adults, as well as children, are vulnerable to racist, homophobic or other forms of hate speech and propaganda, both online and offline, as is recognised by existing regulatory and legal frameworks in many countries. A wide range of vulnerable groups could be affected by addiction to excessive hours playing online games (Khoo et al., 2005) or by accessing (deliberately or otherwise) websites promoting extreme adult pornography, terrorism, suicide and self-harm techniques. Shariff and Gouin (2005) also highlight how the increasing phenomenon of bullying in the online environment typically involves children who know each other, rather than paedophile 'stranger danger'.

It is also helpful to contextualise such concerns for personal safety, for example, safety problems like hate mail have been apparent since the earliest days of the Internet. However, the explosion in Internet use since the emergence of the Web in the 1990s has clearly moved personal safety concerns firmly onto the policy agenda, leading to the relatively recent emergence of safety-related responses.

Security issues concerning the Internet and related ICTs have a longer and more developed history, dating from debates and regulations about the protection of personal privacy in databanks that arose with the emergence of centralised data processing computer systems in the 1960s. The growth since the 1990s of e-commerce and e-government services has further expanded our understanding of Internet-related security matters such as measures for the protection of confidential financial transactions and safeguards against identity theft.

Technical experts also now have extensive experience in dealing with spam and other 'malware', like viruses, spyware and automated software 'bots' introduced to computers without the owner's permission or, often, knowledge. Malware operates under the direction of its creator, for example to undertake fraudulent scams like 'phishing' and 'pharming' to obtain confidential information such as bank details or to carry out distributed denial of service (DDOS) attacks on websites by armies of automated 'botnet zombies' infiltrated into many computers linked to the Internet.

Since the terrorist attack on the US in 2001, the requirements of national security and law enforcement have played a greater role in cybersecurity policy. For example, many governments have sought access even to encrypted confidential information for security purposes and the European Commission has proposed rules on telecommunication data retention that seek to be 'both effective for law enforcement and respectful of rights and business interests'.[1] This indicates how the nature of network-related safety and security problems continually changes as contexts develop.

Rethinking the problems

By helping to clarify not only the distinctions between safety and security perspectives but also their synergies, the conference clearly showed that rethinking the nature of the problems faced can help develop more effective policy responses. Three other key areas where such 'rethinking' could help, are discussed in this section: avoiding the treatment of 'real' and 'virtual' worlds as separate spheres; looking beyond the generic term 'user' to discover how relevant

[1] See: http://europa.eu.int/rapid/searchAction.do (Reference: IP/05/1167, 21 September 2005).

issues actually play out for different people and groups; and understanding how the language used in many media and policy debates is often coloured by deep-rooted emotive psychological, cultural and political influences.

Dissolving the virtual/real dichotomy

There is a tendency in Internet-related discussion to oppose the 'real' world with 'virtual', 'cyber', or 'online' worlds. Many speakers challenged this dichotomisation by emphasising the frequently strong overlap between online and offline experiences. Treating the cyberworld as if it is 'out there' was seen to be unhelpful because it encourages us to look for new, separate solutions to Internet problems without first determining whether we might already have useful experiences or tools in the 'real' world that could help.

An illustration of a desirable, more holistic approach was the showing of a short awareness-raising video advert by the Norwegian Media Authority, created as part of the EU Safer Internet Action Plan.[2] This advert asks teenagers to apply the common sense they apply in their offline experiences to their use of the Internet: 'If it is stupid in the real world, then it's stupid in the cyberworld.'

Many others speakers reiterated the need to avoid treating online experiences in isolation from offline ones. Jim Gamble, Deputy Director General of the UK's National Crime Squad, suggested that the Internet should be regarded as 'just another public place', and that it should be policed accordingly. Shariff and Gouin's (2005) research shows that 'cyber-bullying' using mobile phones and the Internet is strongly connected to bullying and victimisation in the street or playground and reflects unequal power relationships and hierarchies in the classroom. In a similar vein, Mesch's (2005) study of adolescents' use of the Internet revealed that those seeking pornography online are likely to be socially vulnerable on several measures. This reflects a wider overall message that those who are most vulnerable in everyday life could also often be the most vulnerable to online abuse, and should be considered for appropriate help and support wherever possible.

These insights strongly suggest that offline experiences should inform the online. But they do not argue that the real/virtual distinction is irrelevant, as shown by the example of the cross-jurisdictional problems created by the US First Amendment. It is also important to note that the reverse is also true: certain features of cyberspace create genuinely new opportunities and risks with profound impacts on real world activities and lives, such as the ease with which people, information and other resources can be accessed anywhere in the world, both for legitimate and illegitimate reasons.

The holistic approach favoured in this paper emphasises the need to understand real-world contexts in addressing even what appear to be largely technical issues. For example, malware exploits the trust that many people have placed in the

[2] See: http://europa.eu.int/information_society/activities/sip/index_en.htm

technology and in associated protective measures; the more we believe we can trust our computers, the more there is to be gained by those who would exploit us in this way. Strong pressures from ICT-related industry and consumer interests also shape decision-making about technical issues in bodies like the Internet Engineering Task Force (IETF), the large international community of network and ICT designers, operators, vendors and researchers responsible for the evolution of the Internet's architecture (e.g. see Dutton and Peltu 2005).

The overlaps and differences are clearly illustrated by research on children's online experiences reported by Davidson and Martellozzo (2005). Although they found '… the meanings and the motivations behind these [real-world] crimes can be perceived to be the same as those committed in cyberspace' (page 2), they report on page 5 that: 'Children tend to make a distinction between "strangers" and "virtual friends", which means "stranger danger" messages from the real world may be ignored in the virtual.' In other words, at the same time as we recommend that online and offline experiences should not be treated in isolation from each other, we should not forget that for some more vulnerable Internet users, their perception is still of two separate worlds with very different rule-sets.

Making conceptions of 'the user' more concrete

The term 'user' in debates about Internet safety or security may seem to be an aid to making abstract issues more concrete and easier to deal with as it appears to relate problems or counter-measures to particular individuals. However, the opposite may be true. The generic term 'user' can be an abstraction, a way of disguising the fact that little is known about the very different ways in which these issues actually play out for different individuals and groups, such as for particular types of parent, young child, teenager, family, school, etc. Much research evidence was presented at the conference that illuminates online behaviour of certain types of user, but participants generally acknowledged that we still know too little about the ways in which different types of user engage with the Internet.

The evidence presented exposed some common misconceptions. For example, findings from Media@LSE's UK Children Go Online research question the suggestion by some media literacy campaigns that increasing children's understanding of the Internet will help to mitigate some of the risks they might face. Instead, the study found that greater online skill could be associated with greater exposure to online risk (www.children-go-online.net). Similarly, McCarthy and Gaunt (2005) discredited the belief that most adults initiating sexual contact with children online lie about their age.

To be effective, safety and security advice to children, or anyone else, needs to understand the way individuals perceive risks and the influences of contextual social and institutional factors affecting their views and behaviour. Thus, Walker (2005) explains that an investigation in the UK, Spain and Greece discovered that much Internet safety advice to children does not take sufficient account of the emotional context in families and is likely to be ignored by children who feel that an area of independence is being thwarted. Speakers also identified gaps that exist between policy-makers' concerns and the perceptions of people who are said to be at risk. Many people were said to be unaware that computer data can be recovered even after it is thought to have been deleted from a system and Elizabeth France, the UK Telecommunications Ombudsman, reported that only 0.6 percent of consumer concerns raised in 2004/5 with the Office of the Telecommunications Ombudsman (Otelo) related to privacy.

The skills, knowledge and experience of particular users also play a critical role in the effectiveness of attempts to address safety and security problems. For instance, many software suppliers attempt to protect their consumers and the computers where the software runs by providing regular online updates to plug any security gaps that have arisen, either automatically or in response to a prompt from the user. However, discussions at the conference revealed that the efficacy of such an approach will vary across different types of user: some people are irritated by the constant nagging by automatic updates whilst other less experienced users welcome such a service.

The overall lesson seems to be that we should avoid abstract discussion of 'users' in discussing problems of Internet security and safety and, instead, endeavour to make more precise implications clear by considering particular groups. A larger body of empirical social research is needed to help provide policy makers, parents, educationalists and others with more accurate maps of the diverse personal and social profiles of users and contexts of use that shape everyday outcomes tied to the use of the Internet and related ICTs.

The politics of language

The Introduction described the way the terms 'safety' and 'security' carry much emotive and cultural baggage in Internet-related discussions. This kind of 'politics of language' issue can affect the outcomes of debates in which they are used, for example, by emphasising the separateness of otherwise connected issues. This, in turn, can reinforce institutional boundaries and professional divisions that make it harder to deal with the complex and interconnected issues examined at the conference.

The politics of language was strongly evident in a number of conference discussions. Krone (2005), for instance, demonstrated the difficulty of arriving at agreed definitions of terms like 'child pornography' in his analysis of international differences in dealing with child protection. In a debate in a break-out session on terrorism and ICTs concerning the definition of 'cyberterrorism' (see Keith 2005), some participants argued that this is not a meaningful term if 'terrorism' is taken to relate primarily to 'real world' violence; others accepted its meaningfulness in the overlap between real and cyberworlds.

The complexity of the concepts being discussed offer a second sense in which language appears to make a difference to the conduct of debate on the issues at the heart of the conference. This was highlighted in the plenary session titled ‘Privacy, Trust and Security: a Zero-Sum Game?’. At a superficial level, we all seem to understand intuitively the concept of personal privacy, even if we value it in different ways and have different emotional responses to it. On closer investigation, however, the concept of privacy in an Internet age is highly complex. Even seemingly straightforward questions, such as ‘who should have access to my personal data?’, can become highly technical once new security measures are taken into account. For instance, Sandford et al. (2005) explain that it is unclear whether ‘packet sniffing’ techniques that monitor the contents of Internet data packets could legally be undertaken by Internet Service Providers (ISPs), or whether they would count as an infringement of customer data privacy. In such ways, the digitisation of personal information has made the question of privacy inherently more complex at a detailed implementation level, even though broad historical, cultural and psychological values and principles about it remain key emotional drivers. Considerable expertise is therefore required to judge where the balance between personal privacy and information security should lie.

Nevertheless, most of us care enough about privacy to want a say in the decision-making processes about it as the outcomes are likely to affect us greatly. However, the politics of language could cloud informed debate on the subject if its resolution moves away from the grasp of most citizens, at the same time as mass communication and some government and industry rhetoric encourages us to think in terms of simple trade-offs between emotive safety and security values. Thus we are left with a dilemma: the realities underlying the debate on privacy and many other Internet-related safety and security issues are actually too technical to be determined on the basis of popular attachment to certain broad and undefined concepts—but too important to be left entirely in the hands of the ‘techies’ who understand the implementation details.

III Exploring possible responses

A main aim of the conference was to hold a cross-sector, multi-agency conversation about issues of Internet security and safety that could identify potential ways forward. This section summarises some of the wide range of potentially productive options identified.

‘Responses’ versus ‘solutions’

Popular media coverage of many of the more sensational issues discussed at the conference often calls for unrealistic technical or regulatory ‘solutions’ that imply an unproblematic fix to problems, with no further implications, tradeoffs or caveats. This is largely unhelpful, and the conference aimed for a broader approach by seeking to identify a range of practical responses that have a reasonable chance of achieving their aims.

For instance, technology that filters what kind of information and interactions can be accessed from a computer system can sometimes be presented as a solution to the protection of minors. In practice filtering is not in itself a complete answer. The child could have access to other systems or be skilled enough to know how to bypass controls. Filters also raise their own difficulties, such as screening out too much material or material of the wrong kind. In addition, some governments, ISPs and web search engine suppliers fearing state controls may also use filters to suppress free expression and open communication among citizens.

A continuous spiral of technical innovation between those attempting to protect and break security controls means many technical fixes are soon outdated. This occurs between software virus creators and anti-virus programmers or in peer-to-peer (p2p) networks that bypass centralised control by communication directly between individuals' computers.

A key reason for avoiding over-simplistic fixes is that the same capabilities employed for creatively beneficial purposes can also open gateways to much less benign applications. 'The very Internet pathways that convey instant messages, emails, web pages and clicks back and forth also convey executable code [that can contain malware]—and we want it that way', is how Jonathan Zittrain, OII Professor of Internet Governance and Regulation, encapsulated this dilemma during his keynote conference speech.

The most vivid glimpses at the conference of the contrasting potentialities of the Internet came from contributors to the terrorism session who explained how the sophisticated use of the technology by terrorist groups exploits digital technologies' potential for new networked institutional, promotional and financial transformations (e.g. Conway 2005 and Jones 2005). Yet these same Internet capabilities and potential are also applied to achieve very different goals in e-business and e-government management plans.

Reasons to be cheerful: cooperation is possible

Despite concerns that differences of law, politics and culture, and the complex nature of the interrelated problems addressed, would make international and local cooperation on these issues almost impossible, there was a perhaps remarkable degree of optimism expressed about the prospects of achieving progress on key issues.

Many examples of successful cooperation were described at the conference. A few of these are summarised in Table 2, many of which are also discussed elsewhere in the paper.

Table 2. Examples of successful cooperation on Internet security and safety

International	Council of Europe Cybercrime Convention International Action Plan on Spam Enforcement United Nations Commission on International Trade Law (UNCITRAL) Draft Convention on the Use of Electronic Communications in International Contracting of July 2005. www.unis.unvienna.org/unis/pressrels/2005/unisl96.html Ha Noi Agenda on promoting online services and applications among the Association of Southeast Asian Nations (ASEAN). www.aseansec.org/17759.htm OECD (2002) guidelines on the protection of privacy and transborder flows of personal data The Virtual Global Taskforce for cross-border law enforcement
European Union	Safer Internet Action Plan (see Casarosa 2005) Electronic Privacy Directive 2002/58/EC of 12 July 2002 (see Munir 2005) The European Commission's proposed rules on telecommunication data retention, 21 September
National	US CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) Act of 2003 UK Data Protection Act of 1998 US Digital Millennium Copyright Act of 1998 Anti-terrorism legislation in many countries giving increased government access to electronic communication, such as the US Patriot Act of 2001
Self-regulation	Development by ISPs of codes of safety and security practice supported by various tools and services INHOPE worldwide network Internet hotlines to respond to illegal use and content on the Internet. www.inhope.org Microsoft's 'Laws of Identity', a meta-system that seeks to assist identity management on the Internet. www.identityblog.com/stories/2004/12/09/thelaws.html UK mobile phone industry codes of practice for young people and location-aware functionality
Co-regulation	Australia content regulation (see Coroneos 2005) Internet Watch Foundation The European Internet Co-regulation Network (EICN)

Social, economic and institutional levers	Child safety initiatives (e.g. Netsafe and iSafe) Education and mentoring initiatives Treatment of actual and potential offenders (e.g. SAFE project in New Zealand) Social research to understand psychological perceptions and contexts in Internet-related activities Targeting financial resources of malware perpetrators Training data administrator to balance institutional efficiency and legal requirements for digital evidence

Some of the examples in Table 2 required the enactment of new laws or international conventions; others just involved organisations or agencies coming together around common goals to agree new ways of working together. An argument that kept emerging from research findings and related experiences was that quiet pragmatism could often achieve results, but efforts towards over-arching unification are more likely to fail.

Overall, building on existing partnerships was seen as a particularly valuable avenue to pursue. Groups or sectors that are used to working together to deal with long-term ‘offline’ problems have often built on their established relationship to develop common agendas and pragmatic action embracing cyberworlds. NetSafe in New Zealand and iSafe in the USA,[3] for instance, undertake activities in promoting safe use of the Internet and related campaigns that involve networks already used to working together, such as education authorities, schools, children, and family support services.

The Virtual Global Taskforce is an international alliance of law enforcement agencies in Australia, England, Wales, Canada and the US together with Interpol (www.virtualglobaltaskforce.com). It exemplifies the type of more formal initiative that was seen by many at the conference to make a real practical difference by creating new institutional alliances between agencies, some of which might have previously just cooperated informally. This initiative did not require new legislation to be introduced for real progress to be made, allowing Taskforce members to focus on updating traditional policing methods to take account of the Internet as an important new public space.

As indicated in Table 2, there are also a number of higher-level international agreements, such as the Council of Europe Cybercrime Convention,[4] which covers areas like computer-related fraud, child pornography and law enforcement assistance between states; the International Action Plan on Spam Enforcement[5] involving many agencies from about 15 countries seeking to develop effective responses to spam; and the Ha Noi Agenda, which is part of wider ASEAN

[3] See: www.netsafe.org.nz regarding NetSafe and www.isafe.org on iSafe America Inc.

[4] See: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[5] See: www.ftc.gov/bcp/conline/edcams/spam/zombie/

cooperation on e-commerce and other ICT-related activities. Support in promoting research and activities that address the issues discussed at the conference is also important, such as EU's Safer Internet Action Plan.[6]

Some critics suggested that higher-level international agreements rarely produce tangible results. However, such arrangements at least show that international agreement on measures to address security or safety problems is possible. Critics also argue that it may be relatively easy to work with partners in countries who share similar goals and values, but that it is far tougher (and perhaps more urgent) to find a way of working with states unwilling to take action to enhance Internet-related safety and security. A counter argument is that moves towards international cooperation and debate can help to persuade countries with emergent ICT infrastructures, and those who are already digital crime havens, to appreciate the benefits of agreeing an international position.

The influence of ideology and political culture

The bringing together of individuals with a diverse range of ideological positions was a major strength of the conference, as it reflects the reality in which Internet-related policy is typically made. Such diversity reflects not only the left–right axis of traditional party politics, but also a distinctive ideological spectrum that has accompanied the rise of the Internet. This typically contrasts interventionist or regulatory principles with libertarian, non-interventionist ones. For example, the Electronic Frontier Foundation describes itself as 'a group of 'passionate people—lawyers, technologists, volunteers, and visionaries' who 'challenge legislation that threatens to put a price on what is invaluable; to control what must remain boundless … Because being able to share ideas and information is the reason the Web was created in the first place' (www.eff.org).

Busch (2005) illustrates how ideological and cultural contexts shape the outcomes of international collaboration, in his analysis of two cases of US–EU negotiations relating to transborder data flows: the 'Safe Harbor' agreement, which reached a compromise that accommodated both US and EU perspectives; and the handling of air flight passenger name records, which he said seems to have resulted in a substantial acceptance of US demands.

Ideological positions also affect apparently 'neutral' technical developments. The Internet's design, engineering and development principles were strongly influenced by the social libertarian culture of the academic environments from which it initially emerged. These values became manifest in the Internet's open architecture, which is designed to promote the free flow of information end-to-end across a network whose links are valued as 'mere conduits' of data in order to leave users and their systems at the end points to generate their own collaborative creativity (e.g. see Dutton and Peltu 2005).

[6] See: http://europa.eu.int/information_society/activities/sip/index_en.htm

Important themes at the conference were the continuing influence of these initial design choices and the embedding of enduring safety and security threats in past and current patterns and habits of Internet usage. This raised an intriguing question: if the Internet has shaped the emergence of some security threats, to what extent should we look to it to provide some possible defences? OII Chair of Internet Governance and Regulation Jonathan Zittrain suggested an answer by setting out key policy choices that face us in the future development of the Internet (Table 3).

Table 3. Possible future directions in Internet development

Focus	Why?	Why not?
More alert users	More informed users supported by better tools can enhance their PCs' security	Procedures and tools to protect PCs likely to be too complex and inefficient to operate
More alert PCs	Involving expert suppliers in helping to monitor and update security controls on PCs ensures security risks are quickly dealt with	Control by a third party limits freedom to use systems with creative potential. Could lead to more restricted PCs, and raises concerns about transparency
A more alert Internet	If the Internet 'middle' can help to establish the reputation of software authors (e.g. to block DDOS zombies) this helps users and the network itself	Breaks key design principle on which Internet creativity has blossomed by interfering with control by users at the end-points of the network
Balancing user and architectural responsibilities and controls	More secure support from Internet 'middle' while enabling users to choose risk level supported by their own PC	Would still remove control from users

Source: Based on Jonathan Zittrain's Keynote Speech at OII Conference. http://webcast.oii.ox.ac.uk/?view=Webcast&ID=20050927_89

Zittrain argued that balancing the Internet's beneficial creative potential and providing protection against its harsher risks is most likely to be achieved by exploring the bottom two approaches in Table 3. He welcomed any move towards a more alert Internet that provides 'a meaningful, non-monopolistic way' of enabling users to decide the level of security they want on their own PC. This would enable an inexperienced user to choose a 'dumb appliance' ultra-safe mode in which the Internet would offer high but inflexible security controls, while allowing a more expert user on the same system to switch the PC to a lower security mode offering a similar level of creative control to that which has generated the many applications and information sources that—for better and worse—has formed the basis of the Internet's global success. This again highlighted the importance of not regarding ICT users and consumers as a single undifferentiated group.

Zittrain acknowledged the continuing influence of the Internet's early ideological stance when he noted that the very notion of a more alert Internet would be highly controversial because it would overturn the fundamental open design principles that oppose any central infrastructure 'interference' in the flow of data packets along Internet communication conduits. However, he reflected the views expressed by others at the conference in arguing that the establishment of some boundaries to the Internet's openness is likely to be necessary in order to avoid security and safety hazards eventually overwhelming the enormous beneficial potential of the technology.

Regulatory options and accountability

Examples of collaboration that bring together industry, regulators and other stakeholders were frequently highlighted at the conference. Self- and co-regulatory initiatives may involve carrots and sticks to get different groups to the table, for example industry may become more proactive in addressing a particular issue if there is otherwise a clear threat of government intervention. However, such multi-stakeholder relationships can be highly effective once they are established. An example is the UK mobile phone operators group that came together to establish a Code of Practice for access to mobile content by under-18s and subsequently developed a Code for 'passive location services'.[7]

Coroneos (2005) explains how, when the Internet industry in Australia was presented in 1999 with the prospect of mandatory filtering of Internet content to protect children, it responded by developing codes of practice that are legally enforceable. This requires ISPs to provide tools and information to enable customers to control content accessible in homes. In the UK, the Internet Watch Foundation was formed in 1996 by agreement between the government, police and ISPs to tackle the distribution of child abuse images online. Its activities such as a 'notice and take down' service asking ISPs in the UK to remove potentially illegal content has resulted in less than 1 percent of potentially illegal online child abuse content being hosted in the UK in 2003, down from 18 percent in 1997 (www.iwf.org.uk). ISPs in many other countries have developed codes of practice relating to Internet safety and security (e.g. see the website of EuroISPA, the pan-European association of ISPs, at www.euroispa.org).

Casarosa's (2005) analysis of the European regulatory approach to cybersafety indicates that self- and co-regulation initiatives are likely to be most effective if they are incorporated into a clear and coherent regulatory framework. Lievens et al. (2005) identify key issues that such a framework needs to address, such as: the rights of the child, freedom of expression, privacy, protection of minors, open cross-border communications, and e-commerce.

[7] See: www.orange.co.uk/about/regulatory_affairs.html

Many contributors to the conference emphasised that current regulatory approaches were generally not flexible enough to deter, detect and prosecute Internet security attacks. New measures suggested included: allowing 'hacking-back' to attack the sender of malware (Kesan and Majuca 2005), making developers of software or operating systems liable for security weaknesses, or asking ISPs to take on more responsibility for network security.

Some also argue that users should be more accountable if they run poorly secured systems that open doors to allow malware to enter the network, and some ISPs already cut off subscribers who they suspect of such lapses. However, such user liability could introduce penalties many users will find unacceptable and are likely to require stricter security tools and procedures that are difficult, cumbersome and inefficient to operate—and so will probably not be sustainable.

A number of speakers emphasised that, in practice, the direct regulation of young people's use of the Internet is in the hands of parents, teachers and others in their social environments. In the politics of regulatory language, however, 'Internet co-regulation' typically refers to collaboration involving just government and industry. The importance of broadening policies and discussion about co-regulation to include stakeholders other than government and industry has begun to be recognised at national and international levels, for instance through the EICN, the European Internet Co-regulation Network (http://network.foruminternet.org).

Social, economic and institutional levers

In addition to the kinds of regulatory responses outlined above, there are a variety of potentially practical strategies involving the identification and use of broader levers capable of addressing the complex social origins of problems that may otherwise be ignored. Initiatives like the codes of practice developed in Australia and the UK and actions by many ISPs to restrict material available to minors may be a valuable aid to reduce risks to children, but do not address the kind of underlying real-world factors identified by Mesch (2005) as affecting the vulnerability of some teenagers.

This indicates that responses to the problems examined at the conference should prioritise the use of wider social, economic and institutional levers, rather than simply concentrating on regulatory or technical responses. This might include where appropriate, policies relating to education and psychological, health and welfare support. Such an approach to the more imaginative use of social levers was outlined in McCarthy and Gaunt's (2005) call for more integrated responses to dealing with online sex offenders, including treatment and prevention as in the work of SAFE in New Zealand (www.safenetwork.co.nz).

Outside child safety issues, the reaction in many countries to terrorist attacks on the US in 2001 shows how fear can be a powerful social lever in changing attitudes, which in turn will influence which policies are seen as acceptable. The media has also played an influential role in heightening fears about Internet-related paedophile and pornography risks to children and the security threats to PCs and websites.

Public discourse, as reflected in, or created by, the mass media, often sends out conflicting messages about the Internet. On the one hand, the Internet and related ICTs are often portrayed in terms of safety and security 'horror' stories, with governments sometimes gaining political capital by being seen to respond to public concerns even where no significant new risk is evident. On the other hand, there are frequent promotions in media editorials and advertisements of the technologies' life-enhancing potential, including as an essential aid to the education, enlightenment and enjoyment of children and young people. The influence of such conflicting messages makes the role of parents, teachers and others responsible for children particularly difficult. Trying to control access to the Internet too heavy-handedly can lead to accusations that access to potentially beneficial capabilities is unfairly and unnecessarily blocked. Such an approach may also be self-defeating: younger people often know better than their elders how to get access to the online services that attract them, even when attempts are made to block access.

It may be hoped that responsible journalism can be encouraged to provide more informed and balanced media coverage, but entrenched journalistic practices make this unrealistic for the majority of the most popular mass media. In a break-out conference session examining NGO experiences of implementing child safety initiatives, some comments by participants indicated that what is reported is often not solely the responsibility of journalists. Some practitioners said they try to achieve an appropriate balance when dealing with the media. Others acknowledged that the contexts in which the media operate frequently mean the best way of gaining coverage and widespread public and political support for a new safety initiative is to provide a sensational story. Other players may also have conflicting interests when it comes to getting a media message across: the ICT industry may have a vested interest in either downplaying or heavily emphasising a risk, depending on whether or not their products are risk-generators or risk-reducers, whilst members of government can gain political capital by responding to, rather than rebuffing public concerns, even where no significant new risk is evident.

Other social levers mentioned at the conference included aspects dressed in the language of rights and responsibilities. Delegates were asked whether or not Internet use should be portrayed as a right or a privilege, with parallels drawn between Internet use and driving a car. In the latter case, training and proof of proficiency are needed before a license is granted. How desirable or feasible would it be for the Internet to follow a similar course?

Economic and financial levers can act as a way of incentivising desired behaviour or to punish unacceptable practices. This is evident in competitive pressures on ISPs to provide high levels of personal safety protection and software providers to improve their security; some companies have even sought to build their brand based on such issues. It is also possible to impose penalties on sources of finance and gain related to malware, DDOS and other cybercriminal actions.

Institutional levers may also need to be brought into play to achieve a desired objective. For instance, Endicott-Popovsky et al. (2005) highlighted a growing need for 'network forensic readiness' to ensure digital evidence is available to help investigate and prosecute online and offline criminal actions (see also Burnett and af Segerstad 2005). Organisational guidelines and training can help network administrators to balance the institutional need to restore an attacked network as quickly as possible with the vital need to retain digital forensic data to assist law enforcement.

A framework that can help to assess different response options is a key theme in the next, concluding section.

Conclusions: reducing harm by increasing cooperation

This section summarises significant opportunities and challenges identified at the conference, including a potentially fruitful shift in the way debates and policy-making in Internet-related safety and security might be framed in the future.

Joined-up thinking to seize opportunities for cooperation

The discussion of issues relating to both the safe personal use of the Internet and Internet security was a central motivation for the conference. This was fully justified by the outcomes outlined in this paper, which indicate that further cooperation and collaboration is likely to be valuable. For example, security experts could learn from child-safety NGOs' experience of promoting public education, whilst those concerned with safety need to be aware of technical and regulatory developments that affect what the Internet will look like and how we can use it in the future.

Recognising that our activities online have their roots in offline behaviour and experiences should encourage us to explore whether the tools and measures we use to deal with offline manifestations of problems, such as bullying or abuse, could also help us to deal with similar problems online. This holistic approach also emphasises the importance of giving as much attention to the contexts in which the Internet is used as the technologies underlying the technology, especially in paying more detailed attention to the perceptions, motivations and anxieties of specific users rather than generic reference to undifferentiated user groups. Government and other policy makers should therefore consider the online world as part of public space, where responses to problems regarding safety and security in the online and offline world should be dealt with in an integrated way through more 'joined-up thinking' between and across agencies, departments, sectors, and other interested parties. It was also emphasised that a pragmatic, step-by-step approach is usually a better way to make advances than waiting for the perfect solution.

With realistic goals and the willingness of ground-level organisations to communicate with each other, further collaboration could be usefully explored in specific contexts to deal with specific issues, including efforts to see how established partnerships in the offline world could be mobilised around Internet safety or security issues. A more imaginative use of a wider range of responses could see a significant improvement in addressing the problems discussed.

Challenges to be faced

As well as reasons to be cheerful, the conference highlighted several areas where unanswered questions may slow progress. These challenges should be the focus of further research and discussion across all sectors.

Not all participants agreed that such incrementally positive steps were significant enough from an overall perspective. ICTs' double-edged nature suggests that even 'muddling through' with relatively sure-footed progress is unlikely to lead to the precise outcomes targeted by policy makers. The existence of 'digital criminal havens' in regimes that do not cooperate in international conventions or institutional codes of practice illustrates a key potential gap in the step-by-step approach. However, international and local debate and economic or political incentives could be targeted at convincing such states that cooperation is important. Providing support for nations with emerging Internet and ICT infrastructures to ensure they do not become the digital criminal havens of the future is a particularly important global policy issue.

Despite such difficulties, the value of taking relatively small practical steps where possible can be immense. For instance, Dutton and Peltu (2005) have shown how socioeconomic and institutional outcomes emerge from the taking of numerous local decisions by a multitude of actors in different interrelated arenas, such as the kinds of child protection, cybersecurity, regulatory, ICT industry and education arenas represented at the conference and in this paper.

One of the main practical barriers to progress was seen by many to be institutional inertia. This causes many organisations that could play a positive role to fail to fully engage with online manifestations of problems they already address offline, perhaps through ignorance, habit, rigid procedure or even fear. Those who have successfully made that transition may need to help others learn how this can be achieved, without threatening existing successes.

In order to engage as many stakeholders as possible in meaningful discussion on the important topics covered at the conference, more effort should be made to help people understand what information rights and responsibilities they bear, and the implications of these in their everyday lives. This requires addressing 'politics of language' issues highlighted earlier, including the responsibility of communication media, which can strongly shape the way people assess actual risks and potential responses. Discussion on the distancing effect that can be introduced by a generic use of the term 'user' illustrates that these communication barriers exist in expert discussion, not just the mass media.

The impact of the convergence of digital technologies into multimedia ICT products and services cannot be under-estimated, for instance in relation to its impact on intellectual property rights in digital media (e.g. see Lessig 2004). Such technologies have already revolutionised telecommunications and media industries and transformed many aspects of modern living around the world. Future developments could include 'pervasive computing' networks of wireless and wired ICT-based products and services, including sensors embedded in the environment, that could significantly extend capabilities for the continuous gathering of information on an individual's whereabouts and actions. Continuing social, regulatory and technical research at micro and macro levels to help policy keep pace with future developments of fast-changing technologies and their wider social, economic and institutional implications is therefore essential to informed decision making.

Seeking a balanced harm reduction framework

In his summary of what he saw as key themes of the conference, Bill Dutton referred to a story by Mark Twain, *The Danger of Lying in Bed.*[8] This starts out with a concern for rail safety, but the author found from death statistics that most people died in bed and that few people died on trains. So, he ironically advised people to avoid lying in bed if they want to have a long life. As Dutton noted, this does not mean that concern about rail safety is misplaced, but it does show that perceptions of risk are often very different to actual risk. This brought to the fore an important, often implicit, thread from the conference about the value of moving the discourse and analysis of Internet-related safety and security towards the kinds of understanding of 'harm reduction' that is common in disciplines related to the management of risk in hazardous industrial activities, healthcare, transport and many other areas (e.g. see Royal Society 1992).

Risk assessment approaches can help to put specific risks, like online threats to children, in a balanced context, and risk perception studies can provide insights into the psychological and social influences on how people actually view the risks they encounter, including the ways in which risk is reported in the media and debated in public (e.g. see Pidgeon et al., 2005). This would help in formulating polices geared to acceptable levels of risk, where what 'acceptable' means requires an understanding of psychological and social contexts as well as technical capabilities. A key outcome of a shift towards risk assessment and

[8] See: www.mtwain.com/The_Danger_Of_Lying_In_Bed/0.html

perception approaches for Internet safety and security issues could be a greater focus on harm reduction rather than unrealistic risk elimination. References were made during conference discussions to the relevance to Internet-related safety campaigns of harm reduction approaches similar to those applied in drug education campaigns.

In tune with this paper's emphasis on possible responses rather than unproblematic solutions or recommendation, this is not to argue for a wholesale adoption of any particular risk management method. Instead, it suggests there could be a value in considering whether certain risk management approaches and discourses could help to achieve key ideas highlighted in this paper, such as a more holistic approach to Internet-related safety and security. Such a framework cannot provide an 'objective' answer to the question of how much risk we should accept ourselves or allow for those for whom we have responsibility, as the variables involved are too complex and outcomes too unpredictable. However, a key aim of future collaboration between the safety and security communities represented at the conference could be to draw on risk management ideas and discourse, including training in relevant skills, to develop a framework that supports a more informed and transparent approach to balancing the cyber-rights and responsibilities we must all bear.

References

General

Dutton, W.H. and Peltu, M. (2005) The Emerging Internet Governance Mosaic: Connecting the Pieces. OII Forum Discussion Paper No. 5 (Oxford Internet Institute: Oxford). www.oii.ox.ac.uk/resources/publications/fd5.pdf

Lessig, L. (2004) Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity (Penguin: New York).

OECD (2002) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD: Paris).

Pidgeon, N.F., Kasperson, R.K. and Slovic, P. (eds) (2003) The Social Amplification of Risk (CUP: Cambridge).

Royal Society (1992) Risk: Analysis, Perception and Management (Royal Society: London).

Conference papers

The following papers, prepared for the *Safety and Security in a Networked World* conference (Oxford Internet Institute, 8-10 September 2005), are available from: www.oii.ox.ac.uk/research/cybersafety/?view=papers

Balfour, C. (2005) A Journey of Social Change: Turning Government Digital Strategy into CyberSafe Local School Practice.

Brunskill, B. (2005) Safety and Security Challenges posed by the delivery of e-government services.

Burnett, R. and af Segerstad, Y.H. (2005) The SMS Murder Mystery: The Dark Side of Technology.

Busch, A. (2005) The Politics of Transborder Data Flows: Competing Values, Interests, and Institutions.

Casarosa, F. (2005) A safer Internet for children: the European regulatory approach, with evidence from Italy and United Kingdom.

Conway, M. (2005) Terrorist 'Use' of the Internet and Fighting Back.

Coroneos, P. (2005) Industry Facilitated End User Empowerment within a Co-regulatory Environment: The History and Practice of Online Content Regulation in Australia.

Davidson, J. and Martellozzo, E. (2005) Protecting Children From Sex Offenders Online: When Strangers Become 'Virtual Friends'.

Endicott-Popovsky, B., Ryan, D. and Frincke, D. (2005) The New Zealand Hacker Case: A Post Mortem.

Gow, G.A. (2005) Prepaid Mobile Phones: the Anonymity Question.

Gracey, M. (2005) Censorship or Common Sense?

Hardman, H. (2005) (Self-?) Censorship of the Internet in Russia.

Harré, D. (2005) Implementing an Integrated National Cybersafety Programme for the Compulsory School Sector.

Jones, C.W. (2005) Online Impression Management: Case Study of Extremist Web Sites and their Credibility Enhancement Strategies.

Keith, S. (2005) Fear-mongering or Fact: The Construction of 'cyber-terrorism' in US, UK, and Canadian News Media.

Kesan, J.P. and Majuca, R.P. (2005) Hacking Back: Optimal Use of Self-Defense in Cyberspace.

Khoo, A., Hawkins, R. and Voon, F. (2005) Children's Use of the Internet, Including Access via Mobile Phones.

Krone, T. (2005) Protecting Children from Online Sexual Exploitation: In Search of a Standard.

Lievens, E., Valcke, P. and Stevens, D. (2005) Protecting Minors Against Harmful Media Content: Towards a Regulatory Checklist.

Lips, M., Organ, J. and Taylor, J. (2005) Electronic Government: Towards New Forms of Authentication, Citizenship and Governance.

McCarthy, J. and Gaunt, N. (2005) 'But I Was Only Looking': Serious Challenges for Effective Therapeutic Responses to Online Sexual Offending.

Mesch, G. (2005) Patterns and Characteristics of Israeli Adolescent Internet Users that Frequently Visit Pornographic Sites.

Munir, A.B. (2005) Retention of Communications Data: Security vs Privacy.

Rundle, M. and Laurie, B. (2005) Identity Management as a Cybersecurity Case Study.

Sandford, P., Parish, D.J. and Sandford, J.M. (2005) Identifying Internet Abuse in ISP Networks: Practical, Technical and Legal Issues.

Shariff, S. and Gouin, R. (2005) Cyber-bullying: Balancing Student Safety, Freedom of Expression and Learning in a Virtual School Environment.

Thomas, D. (2005) Cybersecurity and Domestic Surveillance or: Why 'Trusted Computing' Shouldn't Be.

Walker, R. (2005) Young People Using the Internet.

Wright, A. (2005) Coregulation of Fixed and Mobile Internet Content.

Glossary

Automatic update: Automatic online updating of software products, for example to patch-up known errors or to add new virus or spyware profiles to protection software.

Bot: Automated software robots (e.g. a smart e-mail filter that adapts to each user's preferences or 'spiders' sent by a search engine to detect the latest information on Websites).

Botnet: A collection of bots, typically acting as zombies in a DDOS attack.

Chat room: Online space where people can interact with each other in real time using virtual names that allow real identities to be hidden.

DDOS: Distributed Denial of Service, typically using numerous zombie computers.

Denial of service: Attack on a Website or other computer or network service with the aim of disrupting the service provided by that site.

Digital dossiers: The accumulation over a lifetime of digitally recorded data (e.g. including emails, mobile phone call records, photographs and school, medical, bank and other records).

Filter: A system that blocks the receipt of certain categories of information or access (e.g. to block spam email or prevent a computer used by a child from accessing certain Websites).

Grooming: The way a paedophile seeks to be build trust with a child (e.g. by adopting a supportive persona in a chat room).

Hacking: Unauthorised and illegal access to computer networks and systems.

ISP: Internet Service Provider.

Malware: Malicious content infiltrated onto computers (e.g. a virus or worm sent via spam).

Packet sniffing: Packet sniffing systems are computer software or hardware that can monitor and intercept ‘packets’ of data passing over a digital network.

Peer-to-peer: A peer-to-peer (or P2P) computer network is one which relies primarily on the bandwidth and computing power of the network’s participants rather than on central servers. Files containing audio or video content can similarly be passed directly between computers or mobile phones using such P2P technology.

Pharming: An attempt by hackers to redirect a website’s traffic to a fraudulent website, often with a view to stealing sensitive personal information such as bank details.

Phishing: An attempt to fraudulently acquire sensitive personal information such as bank details by the sending of fake e-mails or instant messages which appear to be from an organisation or individual familiar to the recipient.

Spam: Bulk, unsolicited messages which are sent via electronic messaging systems to a large number of recipients, often with a view to selling products or obtaining money. E-mail spam is the most widely recognised form, but the term applies in other media, such as instant messaging or text messaging.

Spyware: Malware that enters a computer without explicit permission from its owner, and often without the user’s knowledge, and then sends information from that computer to the spyware’s owner (e.g. transmitting all keystrokes made on the computer being spied on).

Virus: A self-replicating computer programme that spreads by inserting copies of itself into code or documents on others’ machines.

Worm: A self-replicating computer programme which, unlike a computer virus, is self-contained and does not need to be part of another computer programme to spread.

Zombie: Software placed on a computer without the owner’s knowledge, which can make it a slave to the zombie’s controller. See also botnets.