Cyber Trust and Crime Prevention: A Synthesis of the State-of-the-Art Science Reviews

Brian Collins and Robin Mansell **
RMCS Cranfield University and London School of Economics and Political Science

While the Office of Science and Technology commissioned this report, the views are those of the authors, are independent of Government and do not constitute Government policy.

EXECUTIVE SUMMARY

This report provides a synthesis of theoretical and empirical work in the sciences and social sciences that indicates the drivers, opportunities, threats, and barriers to the future evolution of cyberspace and the feasibility of crime prevention measures. It is based on 10 state-of-the-art science reviews commissioned by the Foresight Project. Each of the papers highlights the current state of knowledge in selected areas as well as gaps in the evidence base needed to address issues of cyber trust and crime prevention in the future.

Complexity and System Behaviour

The analysis in this report shows that the whole of cyberspace is subject to unpredictable and emergent system behaviour. This gives rise to considerable uncertainty about future developments and this is especially at the interfaces between the components of the system. This review of developments in cyberspace technologies and the social system demonstrates that there will be new opportunities for crime and that strategies to minimise these will involve numerous choices. The solutions for improving cyber trust and crime prevention in a pervasive computing environment will differ from those in use today. New paradigms for cyberspace security, privacy protection, risk assessment and crime prevention will be needed, together with a stronger cross-disciplinary research effort.

Dependable Cyberspace Systems

There is a deployment gap with respect to the software development methods and procedures that support cyberspace. This has major consequences for the dependability of the cyberspace system. Today's methods and procedures for identity verification and authentication are not robust enough to produce trustworthy network infrastructures or trustworthy service applications. A key issue is the level of failure that will be regarded by users as being 'acceptable'.

If future networked computer systems are to attain improved levels of dependability, attention will have to be given to the commercial issues that influence customer willingness to invest in such systems. Achieving improved dependability will require investment in training and education.

** Brian Collins is Professor of Information Systems, Department of Information Systems, Cranfield University, Royal Military College of Science; Robin Mansell holds the Dixons Chair in New Media and the Internet, Department of Media and Communications, London School of Economics and Political Science. This report draws in substantial part on the state-of-the-art science reviews listed in Appendix A. Text from the science reviews, in some instances, is incorporated directly within this report. We are grateful to the authors of the science reviews for permission to draw upon their work in this way. The views incorporated in this synthesis report are not necessarily those of any institution. Professors Collins and Mansell accept full responsibility for the views expressed here and for any errors or omissions.

Means of encouraging this are: 1) continuous upgrading of the qualifications of the labour pool; 2) encouraging awareness of vulnerabilities; 3) supporting cross-disciplinary research, especially on the economic incentives and the links between these incentives and people's perceptions of risk and their willingness to trust networks.

Managing Identity(ies) in Cyberspace

A significant issue for crime prevention is the fact that in cyberspace users currently can choose to maintain their anonymity. This raises new issues concerning the appropriate means of authentication of identity. If the original identification is not conducted properly then there is a risk of error. One means of addressing this is to examine how people respond to specific measures and perceive the trade-offs between intrusions and options for protection, and the respective social benefits and costs of the available options.

Cyberspace Usability, Risk Management and Security

Changes in the design of secure technologies and in social practices and cultural norms of information assurance influence whether strategies to reduce criminal acts or threats arising from changes in information handling procedures will be effective. Empirical research demonstrates that many authentication mechanisms are hard to use or ineffective. Failure to provide users with the necessary understanding, training and motivation encourages human error. Management policies and frameworks will be needed to ensure that security measures are more closely integrated into business processes and design techniques will be needed to foster good security behaviour. As agent-based software is used in an increasingly large number of cyberspace applications, the identification and authentication of software and data objects as well as people will grow in importance.

Cyberspace and Crime Prevention Strategies

Crime prevention strategies will benefit from the development and application of 'criminal opportunity' models. Such models take into account the physical and virtual locations and times when motivated offenders are likely to come into contact with vulnerable crime targets. They provide a means of focusing on the predispositions of potential offenders and on the characteristics of the situation. Research is needed to examine the variety of situations that give rise to criminal opportunities so that the results can be linked to actions supporting security and crime prevention.

Building Forensics into Data Management Tools

A key area for crime prevention is 'ICT Forensics'. Data management tools are being developed, but they do not have incorporated into them the auditability and traceability processes incorporated into them that are necessary for evidence gathering. Such requirements will need to be stated at the outset and collaboration will be needed to agree the necessary principles and standards. Some form of international code of practice will be needed to enable law enforcement agencies to access data to detect crimes and prosecute criminals. Whether the public or private sector should initiate a debate on this topic and who would bear the costs of implementation are urgent questions that need to be answered. In this area the economic incentives that will drive investment in the use of these tools and processes are unclear as is the appropriate balance between evidential - investigative and preventative - computer forensics, an area of particular relevance to business and government. This could be examined in cross-disciplinary research in the area of ICT forensics and cyber-evidence management and is an area of particular relevance to business and government.

Trust and Risk in Cyberspace

Insight into perceptions of risk in cyberspace comes from research into the way members of the public appraise uncertainty and the risks associated with scientific and technological innovations. The social meaning of risks influences the way they are perceived and judgements about

uncertainty. Whereas experts see risks as chains of cause and event, lay people tend to see them in a social context of relationships. Perceived risk may be amplified or attenuated depending on a large number of social and technical factors. Research frameworks are available that could be applied to examine why some risks associated with cyberspace are likely to attract heightened social and political attention. It will also be very important to distinguish between reported perceptions of trust and risk and people's actual behaviour and to acknowledge that the latter often suggests that people are willing to place trust in parts of the socio-technical system even when they report perceptions of heightened risk or low trust.

Research on person-to-person and person-to-system trust points to many variables that influence trust in cyberspace. The way patterns of networked social relations foster social capital and 'webs' or 'networks of trust' in virtual communities could be examined to suggest new means of crime prevention. In research on system-to-system level trust, conducted using game-theoretic approaches, it is assumed that an agent's decision to play in a game involves trust that actor(s) will behave as expected. Economic analysis in this area suggests that it may be the distribution, rather than the level, of trust that supports the setting of priorities for establishing trust relationships and a structure for negotiating the distribution of liabilities arising from cyberspace interactions. Further work will be needed to understand the implications for cyberspace markets.

There are divided views about the ethical justification for interventions in cyberspace that would seek to limit the way the Internet facilitates 'playing' with identities. Discussion in generic open forums is difficult because different meanings become attached to the perceptions of risk and danger. Judgements about whether there are grounds for crime protection strategies will need to take account of the trade-offs between individual privacy and the benefits of greater collective security.

Although citizens need to be better informed about cyber trust and crime prevention, as in other instances where there is uncertainty, there is a danger of amplifying the perceived threats and dangers. As awareness of cyberspace risk and vulnerability continues to spread, it will be important to foster debate in ways that enable consideration of the feasibility and appropriateness of proposed actions to limit crime.

New Cyberspace Technologies and Trust

Two key areas of technological development are software agent-based systems and knowledge technologies and the semantic web. Protocols will be needed to ensure that the software and human agents tell the truth and interact honestly with each other. The various tactics for fostering trust have costs and benefits and they must be combined with effective trust management strategies. The available means of fostering trust raise questions about identity, anonymity and privacy and about the maintenance of the content and provenance of information. Trust in the Internet seems to be enhanced as people learn more about cyberspace, but experience over time may create new uncertainties and perceptions of risk. The underlying social dynamics and learning processes that are involved in cyberspace risk perception and trusting behaviour need to be examined systematically and on a comparative basis internationally.

Cyberspace Market Evolution

The development of cyberspace is a global phenomenon and effective monitoring of markets and legislative and policy environments is essential for effective crime prevention strategies. In cyberspace markets firms may use or misuse trust and it is theoretically possible for these markets to lock-in to a 'low trust equilibrium'. Demand for security solutions is influenced by the costs of switching between cyberspace security products on the market. Economic analysis suggests that the sustainability of trust relationships in evolving cyberspace markets may actually depend on asymmetries among the participants. Measures to reduce information asymmetries or to enhance the security of cyberspace may undermine certain kinds of trusting behaviour. Incentives for investing in the deployment of more trustworthy networks and applications will depend on the

dynamics of the market and research will be needed, particularly on how the market will evolve in those areas where there are few suppliers.

Policy Context and Privacy

Many different international instruments, national legislative approaches and self-regulatory or voluntary tools are in use to address commercial and social issues including privacy protection. Technical solutions for communicating and transacting using rigorous authentication may eventually provide a foundation for greater trust in cyberspace, but they will also create new threats. Encouraging the development of new principles and practices to complement existing security and privacy guidelines may be one means of fostering good cyberspace behaviour.

Issues of balance are often a central feature of policy responses to the need for privacy protection. The conventional privacy paradigm rests on a concept of society as comprising relatively autonomous individuals. This view is criticised by those who believe that insufficient weight is given to collective or community interests. The distributional issues and equity issues in this area need to be examined to assess who enjoys what privacy and why. Inequalities in the distribution of privacy protection could be treated as a social policy issue and consideration should be given to whether inequalities are justified and whether public policy could alter them.

The overriding goal with respect to cyber trust and crime prevention is to reduce crime to tolerable levels without incurring unacceptable privacy intrusions. The development of privacy impact assessment methodologies could help to resolve tensions between individual privacy and collective security and to assess the adequacy and enforceability of data protection and freedom of information legislation. It is clear that the resolution of ethical issues in the contexts where privacy issues come to the fore will play a key role in determining the acceptability of crime prevention measures.

Lessons for the Future

There are many uncertainties about the trade-offs that will accompany human and technical measures to develop a more dependable and secure cyberspace system that will help to minimise the risk of new criminal opportunities. In the light of the relatively weak scientific evidence in important areas concerning cyber trust and crime prevention, there will be a need to consider the ethical positions associated with crime prevention measures and to draw inferences about their impact. Critical reasoning can be applied to reach such judgements – subject to review as new evidence accumulates - about ‘acceptable’ and ‘unacceptable’ levels of the trustworthiness of the cyberspace system.

Introducing legislative and governance solutions may manage cyberspace risks more effectively, but stifle innovation and competitiveness in the process. No ‘future-proof’ set of measures can be put in place through unilateral action because the relative positions of governments, businesses and citizens are changing and are insufficiently clear. There are research frameworks for developing dependable software engineering approaches, assessing criminal opportunities, examining the amplification of cyberspace risk, and considering the impact of crime prevention measures on privacy. These could be further developed and interconnected to increase understanding of security measures and crime prevention strategies. Strengthened collaborative and cross-disciplinary research could harness the considerable breadth of expertise that is available in the UK and elsewhere. It will be essential to investigate the central issues, options and choices that will shape the development of cyberspace. New crime prevention measures will be more effective if they are complemented by investment in adequate levels of education and in building awareness of when to trust and not to trust in the cyberspace system.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF BOXES

1 INTRODUCTION

Foresight projects are designed to produce challenging visions of the future with the aim of ensuring that the strategies of today are effective. The Foresight Cyber Trust and Crime Prevention project aims to explore the application and implications of new generations of information and communications technologies (ICTs) in a variety of areas that will present opportunities and challenges for crime prevention in the future. These areas include identity and authenticity, system robustness and dependability, security and information assurance, and privacy and surveillance. All of these raise crucial issues for our understanding of how risk is perceived and trust is fostered within complex social and technical systems. This report provides a synthesis of the existing science base that can offer insight into key interrelationships between the human and technical components of 'cyberspace'.[1]

The aim is to highlight the possible drivers, opportunities, threats, and barriers to the future evolution of cyberspace and to consider the feasibility of crime prevention measures. These will govern future interactions between people and their machines and within a globally networked 'machine'. The future development of cyberspace raises issues that are fundamental to individual and collective human safety and security. It is important to distil lessons from the scientific evidence base and to highlight areas in which there are gaps that could be filled by research and where there is a consensus or controversy about future developments.

Cyberspace is global in its reach. In the UK and elsewhere, many of the solutions for crime prevention could be introduced through public or private initiatives. Many of these solutions, however, require internationally co-ordinated action if they are to be effective. In the UK the science and engineering base is strong in key technical areas as well as with respect to problems and issues that are the concerns of the legal profession, the social sciences and the humanities. This provides a strong basis for leadership internationally.

The evolution of cyberspace is a subject of great controversy. There are divergent views about whether the UK has a competitive advantage in developing technologies that will be trusted by the majority of their users and whether there is a need for government initiatives to ensure the development of trustworthy technologies. There are similarly divergent views about the need to constrain cyberspace developments in order to limit the potential for destructive attack, strengthen collective security, and limit privacy invasive intrusions. The scientific evidence base cannot be applied to resolve all of these controversies. It can, however, be applied to clarify how the human and technical components of cyberspace relate to each other. It can suggest how the interventions in cyberspace by different actors are likely to reverberate throughout the social and technical system.

Cyberspace is a complex human and technical system. The structure of the Internet is favouring fragmentation into many loosely connected cyber-communities that are governed by a range of different principles. This makes the cyberspace system subject to highly unpredictable emergent behaviours and it makes the consequences of efforts to prevent crime very difficult to predict. This is especially so when such efforts are targeted at particularly unstable components of the system.

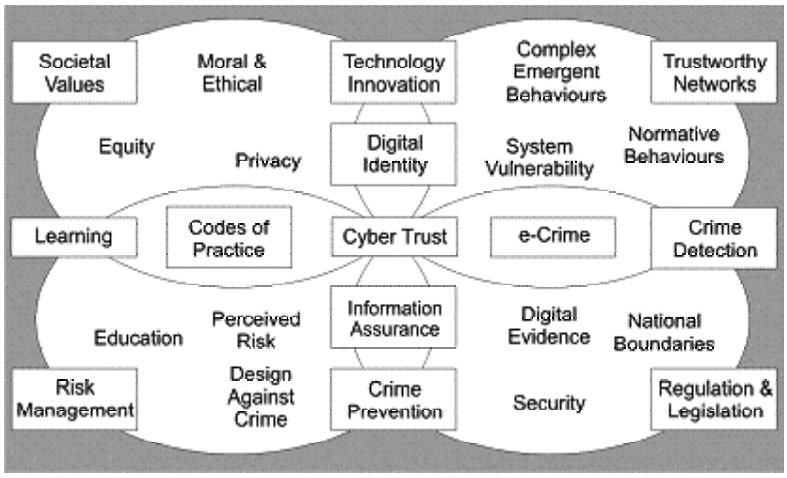
[1] Throughout this report, we refer to 'cyberspace', a term that we define in section 2.0. This term has come to signify all kinds of activities – social and technical – that occur in the electronic environments enabled by digital technologies. Cyberspace is not homogeneous and it is constantly changing. Not only are the technologies deployed in different ways, but the exploitation of them by various social groups differs. For simplicity in this report, we use the term without offering great detail as to the specific technologies or applications (which may embrace open distributed networks and relatively closed networks as well as proprietary and open source software applications).

In some areas, however, there is considerable stability and sufficient understanding of relationships within the system to justify action aimed at improving crime prevention.

One of the key considerations from a perspective that emphasises the relationships between cyber trust and crime prevention, is the development of an understanding of the causes of crime in this new environment. Just as in other areas of crime prevention, it is necessary to assess whether cyberspace developments will give rise to new 'conjunctions of criminal opportunity'.[2] In order to do so, we need to examine features of the components of cyberspace to determine the extent to which people will have greater predispositions to crime, new resources available to them to commit crime and many other factors. At the same time, we need to assess the extent to which those who develop the new cyberspace systems have incentives to adopt measures that will make cyberspace less attractive for criminals and crime promoters (those who make crimes more likely, for example, by providing 'inside information', passwords, tools, incentives and encouragement, etc., or merely by being careless with their own security) wherever they are found.

We address features of the key relationships between the components of cyberspace shown in Figure 1. The figure depicts some of the key components and issue areas in the cyberspace system. Each of these is recursively related to the others, forming a highly complex system that is populated by many different agents, both human and non-human.

Figure 1 Cyber Trust and Crime Prevention - Web of Components



The synthesis of theoretical and empirical research in this report is based on state-of-the-art science reviews (see Appendix A). These reviews provide authoritative peer-reviewed reference material and a foundation for the futures work for the Foresight project. Each of the papers highlights the current state of knowledge in selected areas as well as research that is needed to clarify and build an improved knowledge base in the future.

1.1 Structure of the Report

The next section (*2.0*) provides a brief discussion of the technologies of cyberspace and of the scope and salience of the issues addressed in this report. In *section 3* we consider how those who design computer-based systems understand the processes involved in constructing them as well as the processes of and mechanisms for identifying and authenticating users. Important issues of

2 Ekblom 2002, 2003.

the usability of these mechanisms, the role of cyber-security and risk management, and the future prospects for the trustworthiness of cyberspace area also considered in this section.

The construction and use of cyberspace systems requires many assumptions about the experience and perceptions of trust and risk as cyberspace tools and applications are developed. In *section 4* we examine theories and empirical evidence from a variety of disciplinary perspectives that help to shed light on trust and risk management and on the appropriate models for understanding trust in offline and online environments. We examine the ethical issues and stances that inform divergent and deeply held commitments to the need for more dependable cyberspace.

The discussion in sections 3 and 4 is principally concerned with general trends that apply broadly across the components of the human and technical cyberspace system. In *section 5*, we examine how various models of trust are being applied in two important areas of technical development – software agent-based systems and knowledge technologies and the semantic web. We also consider the available, albeit limited, empirical evidence on the way cyberspace users think about trust.

In *section 6* we examine the economic features and likely dynamics of the evolution of future cyberspace technology and service markets and the interaction of these features with policy measures and the legislative environment.

In *section 7* we reflect on the lessons that can be drawn from existing research about the future context in which crime prevention strategies will evolve. This section highlights gaps in the scientific evidence base and areas in which measures could be taken to develop more trustworthy cyberspace systems that may help to strengthen crime prevention strategies. The overriding concern is to minimise the potential for cyberspace to develop in ways that create new opportunities for physical and cyber crime to occur.

2 CYBER TRUST AND CRIME PREVENTION – SCOPE AND SALIENCE OF THE ISSUES

In this section, we introduce the hardware, software and human systems that comprise cyberspace. We explain why we selected certain key technologies for investigation and why the issues of risk, trust, privacy, security and ethics are critical for crime prevention strategies.

'Technology' may refer to the components of cyberspace such as its hardware and software or it may refer to the social values, norms, practices and institutions of cyberspace. 'Cyberspace' refers to interconnected networks or the space within which electronic communications take place and this term has become interchangeable and merged with the Internet and the World Wide Web and their use by the public.[3] Those who invent, design and implement the information and communication technologies (ICTs) that underpin cyberspace generally agree that much needs to be done to build confidence both in people and in the 'mechanics' of cyberspace.

Analyses of the technical and possible market developments in the field of pervasive computing and trustworthy ICT systems show that some of the technologies are relatively mature and well-understood, but still evolving. Other technologies are immature but reasonably predictable in their evolution, and still others are in the 'blue-skies' research phase.[4] The technologies embrace those used for pattern recognition and cognitive modelling to those supporting network connectivity and broadband access. They include various kinds of software, service platforms and service functionalities.

In this report, we focus particularly on the development of complex software systems and the technologies used to establish identity and to authenticate users of cyberspace. We look specifically at developments in software agent-based computing and knowledge technologies and the semantic web. All of these technologies play a crucial role in the emergence of 'pervasive' or 'ubiquitous' computing and the spread of networks of 'ambient intelligence' (see Box 1). And these technologies play a major role in the extent to which issues of risk, trust, privacy, security and ethical issues become important for crime prevention strategies.

As suggested in Box 1, the majority of current users of cyberspace do not have a good understanding of today's security requirements. As the European Commission's Advisory Group on Information Society Technologies has suggested, the solutions for improving cyber trust and crime prevention in a pervasive computing or ambient intelligence environment are likely to be quite different from those in use today.

The commercial setting in which ICT evolution will occur is subject to the dynamics of the interactions between the players (governments, citizens and consumers, civil society organisations of many kinds, and businesses) and the choices made with respect to regulations, standards, and the role of the market. These, in turn, are strongly influenced by changes in the motivations and actions of those who seek to minimise criminal opportunities through crime prevention and those who seek to exploit emerging technologies to support existing and new forms criminal activity.

3 Skibell 2002; and see Castells 2001; Gibson 1984; Mitchell 1996.

4 Sharpe 2003; Sharpe and Zaba 2004.

Box 1 Ambient Intelligence and the Security Paradigm

'In the ISTAG [Information Society Technology Advisory Group] concept of Ambient Intelligence, intelligence is pervasive and unobtrusive in the environment. The environment is sensitive to the presence of living people in it, and supports their activities. People, physical entities, and their agents and services share this new space, which encompasses both the physical and virtual worlds – the Ambient Intelligent Space – or *AmI Space.*

Security in this space will require solutions very different from those of today's systems which are predicated on relatively stable, well-defined, consistent configurations, contexts, and participants to the security arrangements. … This new paradigm will be characterised by 'conformable' security, in which the degree and nature of security associated with any particular type of action will change over time and with changing circumstances and with changing available information so as to suit the context. … within the existing security paradigm there are significant outstanding problems that inhibit development of information society markets. The majority of potential users of services and products have, at best, a poor understanding of security, which leads to caution and, at worst, severe distrust. They need comprehensible mechanisms in which they can have confidence…'.[5]

In an emergent evolutionary system such as cyberspace where there is an 'arms-race' between offenders and crime preventers, a key strategic issue is 'how to live with it and how to ensure that the balance is tilted as far as possible, for as much of the time as possible, in favour of preventers'.[6]

Crime prevention in the context of cyberspace means reducing the risk of the occurrence of crime and the potential seriousness of crime and disorder events that may occur either in the online or offline world.[7] To achieve this, it is necessary to identify the problems and their causes. Given the relatively recent and rapid development of cyberspace it is not surprising that there are very substantial uncertainties about what future problems will emerge and how they can be tackled. It is clear, however, that cyberspace entails new opportunities for crime because its reliance on networks and communication is such that criminal events may be distributed across geographical space and through time in many new ways. It enables new computer systems and data capture methods that may be vulnerable to attack and, at the same time, offer innovative means of responding to criminal activity. Just as the cyberspace system design itself is evolving and adaptive, giving rise to new forms of criminal opportunity, so are the potential offenders' tactics and strategies.[8] The solutions to the evolutionary arms-race involving cyberspace technologies will undoubtedly lead to new technical design considerations, but their feasibility, in turn, will depend on changing social, cultural, political and economic priorities as well as on a number of crucial ethical considerations.

In a dynamic socio-technical system of this kind, the components of cyberspace often acquire a self-reinforcing structure. The motivations of the different players in society will resolve themselves in particular ways, such that as new ICTs are implemented, parts of the system may become quite stable for a period of time. The significance of this system is that the future use of ICTs will be inextricably bound up with systems that coordinate a large number of technologies within agreed interfaces and standards. These evolve from generation to generation, as the technology shifts and the players act in various ways that change their respective motivations and actions.

5 European Commission, IST Advisory Group 2002, pp. 3-4.

6 Ekblom 1999, p. 47.

7 Ekblom 2003.

8 Ekblom 1997.

At any given time, there will be some dominant organising themes in the spread of cyberspace networks. In 2004, even as the open source software movement was gaining ground, cyberspace technologies were organised largely around corporate and home desktop computing and the 'Wintel' model or Microsoft Windows and Intel microchip model predominated. Mobile communication was in the midst of a transition to its third generation in which data services are delivered alongside voice services. The ICT industry as a whole was undergoing a period of instability and the Internet Protocol (IP) was becoming established as the global networking standard, presenting new issues for pace of innovation throughout the ICT industry and for the smaller and larger ICT producing and using firms. At the content end of the ICT spectrum there was no leading model for the distribution of digital products or for payments. There was much debate about the viability of conventions with respect to intellectual property protection alongside a global information commons. In the commercial domains of cyberspace, many new electronic services were emerging and gaining market traction, suggesting that a relatively stable structure will emerge.

Analysis of the potential threats to human safety and security in a future pervasive cyberspace environment is complicated by uncertainty about how the public will perceive its risks, whether or not they perceive it as trustworthy, and whether they behave as if it is trustworthy. The public perception of risk has been examined in cases of risks from exposure to technological dangers such as radioactivity, pollution and other hazards. Relatively little attention has been given to the analysis of public perceptions of cyberspace risk, despite the considerable work on risk and financial markets in the business community. Much of the information people receive about cyberspace risk comes from the media and a growing variety of Internet-based sources of imagery and symbols. All of this information is transformed by multiple actors and interpreted in different ways producing consequences that we are only beginning to understand.[9]

The concepts of trust and risk have become increasingly important for understanding life within a complex socio-technical system.[10] Today's socio-technical systems are being created in an environment of chance and risk. This environment embraces interdependent systems of production, consumption, governance and technology control. When science and technology create new knowledge – in this case, the production of cyberspace - risks are identified and appraised through human attention and judgement. This is giving rise to new perceptions of risk and to new meanings and interpretations of developments in cyberspace.[11] People will assess the risks as being more or less serious depending upon how they weight the consequences. This has substantial implications for the viability of crime prevention strategies.

Identification of a threat or danger associated with cyberspace and the appraisal of its possible consequences also raises ethical issues and the need to consider how new criminal opportunities give rise to the need for new principles, responsibility and accountabilities.[12] There is considerable uncertainty about how trust in the offline world is being transferred into cyberspace and about the trustworthiness of the components of the cyberspace system. Problems and perceived dangers may be seen as a failure either of the technical system or as a failure of the system designers and users to take steps to prevent crime or vulnerability in the system. It is essential, therefore, to understand the relationships between human factors and risk and trust if a relatively secure cyberspace system is to develop in the future.

9 Jackson et al. 2004.

10 Beck 1992; Giddens 1991; Jackson et al. 2004.

11 Douglas and Wildavsky 1982.

12 Douglas, 1996; Jackson et al. 2004.

In this dynamic socio-technical cyberspace system, issues of trust, the trustworthiness of the emergent system, and the feasibility of crime prevention strategies, need to be considered in the light of questions such as:

- What sorts of cyber trust issues will be of dominant concern – what will be the new kinds of vulnerability and how will the risks of cyberspace be perceived?
- How will the overall structure of the emerging system drive the uptake of cyber trust technologies?
- What kinds of interventions might be made to influence the system's dynamics for the purpose of improving cyber trust and crime prevention?

The technical and human components of cyberspace form a complex emergent system that is subject to periods of instability and stability. Historically, studies of innovation and techno-economic change demonstrate periods of instability and stability as technical and human or social systems interact in new ways. There is no reason to expect the cyberspace system to be different in this respect.[13] Addressing these questions about cyber trust and crime prevention within existing paradigms of trust, security and technology does not suffice to alleviate concerns about potential threats in this environment. In many instances, new frameworks taking into account, as far as possible, the distinctive features of cyberspace are needed.

The range of technologies – technical and social – that is central to the emergent properties of cyberspace is vast. In this report, emphasis is given to those areas and developments that were regarded as being the most important by those consulted during the project. Many of the problems that give rise to perceptions of risk and the insecurity of cyberspace are not new, but crime prevention in the light of cyberspace developments does have some new dimensions. This is particularly so in areas such as the management of digital identities, the processes and tools used to enable reciprocity in cyberspace, and the properties that are required to enable humans to trust in technology systems, i.e. in part, the trustworthiness of such systems. These and related issues are addressed in subsequent sections of this report.

The scope of the issues examined in this report is informed by an analysis of previous studies in closely related areas. Although trust, assurance, security, and dependability, as aspects of cyberspace developments, have been mentioned in previous work, crime prevention itself has not been an explicit focus.[14] In addition, there are differences in the focus of studies of cyberspace-related developments conducted in the US and in Europe as suggested by the following extract.

> 'The US studies tended to be more focused on technological and managerial solutions to the challenges. European studies addressed these issues but discussed more extensively the societal context and had more explicit visions of the desired societal end-state. This perhaps reflects a US focus on managing the risks consequent on market led developments compared to the European attempt to direct and shape these developments. It may also reflect an embedded US view that ICT developments (mainly US-led) are broadly positive, compared to a more sceptical European view that is more concerned about the economic, social and political changes they will entail'.

The European emphasis on the economic, social and political implications of cyberspace technologies is reflected in the state-of-the-art science reviews commissioned for this project. These reviews call for a stronger cross-disciplinary research effort that will build a better foundation for understanding key facets of the technical and human dimensions of cyberspace.[15] The topics

13 Freeman and Louça 2001; Perez 2002.

14 Cremonini et al. 2003, p. 8.

15 Throughout, we use the term cross-disciplinary to encompass those who favour multi-disciplinary or inter-disciplinary research; what we intend is stronger cooperation based upon excellence in research

selected for the state-of-the-art science reviews were chosen by an Expert Panel that advised the project. These topics should not be seen as the only relevant or important ones for the future of cyber trust and crime prevention. The salience of the issues examined in this report also has been confirmed by the Royal Society which has identified identity fraud, trust, the balance between private and public information needs, and the technology-society interface as high priority issues for further research.[16]

Pervasive computing will give rise to the need for new paradigms for managing uncertainty, the perceived and actual risks of cyberspace, and the trustworthiness of the system. The technical and human components of cyberspace form a complex emergent system that is subject to periods of instability and stability. Addressing questions about cyber trust and crime prevention within existing paradigms will not suffice to alleviate concerns about threats in this environment. Cross-disciplinary research on the socio-technical evolution of the cyberspace system is needed to provide improved understanding.

located in many different disciplines.

16 Royal Society 2003.

3 CONSTRUCTING AND USING CYBERSPACE SYSTEMS

In this section, we highlight recent thinking about the way large scale pervasive computing systems are being developed. Software development practices that favour the construction of more dependable systems are examined together with issues of identity and authentication. Research in these areas emphasises technical and human issues and the importance of managing risk and trust in cyberspace.

Technological innovations could affect many elements of the web of interacting and mutually dependent aspects of cyber trust and crime prevention. The dependability of pervasive and complex computing systems has a clear impact on security and on risk. User identification and authentication mechanisms also have an impact on security and, in addition, are tightly bound to tokens, passwords, encryption and the usability of these mechanisms by human agents.

1.2 Towards Trustworthy Pervasive Computer Systems

The UK is not alone in becoming ever more dependent on large networked computer systems yet the dependability of such systems is by no means always satisfactory.[17] Techniques and tools available today make it *possible* to produce complex computer systems that work adequately dependably. However, there is a huge 'deployment gap', with many organisations attempting to produce complex systems and, in particular, software (which is where the complexity of such systems mainly, and appropriately, resides) using technical and management methods which are far from 'best practice'. Even with today's technology we seem to be unable to use the methods and techniques available to us to deploy reliable systems. In the future as we invent even more complex systems, unless there is a major and disruptive change in the way in which we go about deploying systems, the *trustworthiness* of the underlying infrastructure and of the applications that run on it will degrade.[18] Major or radical innovations in technology often require equally major or disruptive changes in practices of system design and implementation.

1.3 Dependability Technologies

Dependability (sometimes and not always usefully termed 'trustworthiness') is the ability to avoid computer system failures that are more frequent or more severe, and outage durations that are longer, than is acceptable. The causes of such failures are termed faults. Acceptance of some level of failure is inescapable. What is at issue is the level of failure that comes to be seen as being unacceptable. This is a complex mix of socio-technical issues that is worthy of further analysis and study. Overstressing the need for a high dependability level when members of society will accept or tolerate a lower one especially to make a system more useable is a very important driver for the design and construction of a complex computer system. It is clear, however, that system failures should be prevented at some level. There are four basic dependability technologies - fault prevention, fault removal and fault tolerance (whose effective combination is crucial), and fault forecasting. These provide the means of assessing progress towards achieving adequate dependability.[19]

A variety of fault prevention and fault removal techniques is currently in use, in some cases, as part of a formal (mathematically-based) design method. However, there is a need to make such methods and their tools easier to use. Fault tolerance is very effectively used for hardware faults and, in some arenas, for software faults. Fault forecasting currently has limitations with regard to large systems and extremely high dependability targets.

17 Royal Academy of Engineering and British Computer Society 2004.

18 Jones and Randell 2004.

19 Jones and Randell 2004.

The problem of deliberate attacks on networked computer systems, and via them on other major infrastructures, by amateur and professional hackers, criminals or well-resourced terrorist groups is already serious and seems certain to grow as systems become more pervasive. Detecting the onset of such attacks is insufficient to ensure system dependability. Means are also needed for maintaining satisfactory service despite such attacks, and for reliably gathering evidence of the attacks if subsequent judicial processes are to be successful.

Because systems are all pervasive, they are and increasingly will be used in the design and testing of new systems and in the support of the operation of 'transactional' systems that the 'end-user' experiences. The reliability or trustworthiness of these other uses is just as important to the 'end-user' systems as the one he or she experiences, and particularly those used in testing. Those used for evidence gathering in support of judicial processes must be at least as provably trustworthy as the end-user system if not more so. The development of complex software relies on state-of-the-art in the software engineering process including the way projects are managed and the choices of technology.

Complex Software Projects and Software Engineering Processes

Complex software projects have certain unique properties that are derived from the fact that they are not governed by physical laws in the way that civil and mechanical engineering projects are. However, complex mechanical and civil engineering projects share a number of properties such as the need to share constraints and dependencies between members of the project team.[20] The management processes that traditionally are applied to software projects involve breaking the total project activity into lines of activity within which there are close interdependencies. These lines of activity are broken down further into sets of tasks that run sequentially. The interdependencies between lines of activity are then also established. This historic approach to the development of software has not been completely successful and there is a need for a fundamental review of the nature of the problem of software engineering and its architecture to develop a more radical approach to new ways of managing this complex set of activities to achieve greater dependability.[21]

In the organisation of software projects teams of people pursue particular lines of activity that are coordinated by an overall project manager. However, as Brooks has pointed out in his seminal book, *The Mythical Man-Month*,[22] the balance between creative work carried out by an individual in pursuit of the task to which he or she has been allocated and the sharing of information about the work with others who are dependent upon him or her becomes an unmanageable process once the team size involved in a line of activity exceeds some 35 to 50 people. In this area technology itself may be able to provide more sophisticated environments for developers to work in, such that the load placed upon them for sharing can be diminished so as to rebalance the time that is available to them to carry out creative work.[23]

Leadership in software engineering centres on the project manager's ability to maintain strong discipline and the sense of direction for the activities involved in the face of demands for unstructured change, movement of team members and reallocation of financial resources. Such leadership qualities will be obtained by a mixture of experience in carrying out a range of tasks within the general field of software engineering and an understanding of the overall activity in a holistic sense. Without strong sustained and high-quality leadership, complex software projects are almost doomed to failure and possibly should never even begin.

---

20 Collins 2004.

21 Collins 2004; Jones and Randell 2004.

22 Brookes 1995.

23 Collins 2004.

A complex software project will be undertaken in order to meet the business needs of the organisation or within a contract to be delivered to an external customer. It is vital not only that the customer is engaged in the development process from its inception to its completion, but also that the project team has well-defined mechanisms that allow the customer to be involved in the project and add value during its lifetime. The way in which the customer engages with the project may be regarded as divisive or incoherent so that the quality of the product is diminished to an unacceptable extent. It is a common experience that project management methodologies with well-defined processes for customer engagement are not always invested in or trusted by customers.

Technical Choices and Software Requirements

In large-scale software projects, there are significant technical choices to be made about how to capture requirements in a systematic way and how to interpret those requirements in such a way that they can be validated against the users' perceptions, and in the concepts of how the software will function when it is installed and operating. In addition, choices must be made of the design language that is used to interpret the requirements in a form from which the programmer can develop code that delivers the functionality that the user requires. There is also the choice of programming language to be made. This must be compatible with the functionality of the project but also with the functionality that is either concurrently developed in other projects or with legacy code with which it has to interoperate, and all have to be compatible with the target platform of both hardware and operating system software on which functionality will eventually reside. Between the development of the code and operation there is a further level of complexity connected with the testing, validation and verification of the code that has been delivered to show that it does indeed meet the requirements of both the user and the system developer (see Box 2).[24]

Box 2 Validating Technical Choices throughout the Project Lifecycle

These complex choices have been written here as if they are linear choices to be taken sequentially. In fact they all should be taken at the start of the project in such a way that an integrated environment for the whole project is defined at the outset. If any major changes are made to the assumptions concerning any of these factors such that for instance a different programming languages is chosen or a new approach to testing is selected, then at least a return to the beginning should be taken conceptually in order to re-verify that the assumptions which were made up to that time, supporting the original choices that were made, are still valid.[25]

This level of complex interdependent processes and tools is not unique to software engineering. Large software projects are not unusual in having changes placed upon them by external factors beyond the project control and frequently the basic assumptions on which the projects are based will not be examined. In such cases it may be necessary to stop the whole project or re-design to accommodate these new developments. This example of applying a professional discipline is an essential part of a successful complex software project. Ideally buyers of such projects should insist on these disciplines being implemented as appropriate. To achieve this, the use of educated and experienced people in the design and implementation of large software projects is an essential part of minimising the risk.

Dependability and Cross-disciplinary Research

Present trends indicate that as ICTs are embedded into almost everything, huge networked computer systems are likely to become pervasive and richly interconnected and required to function essentially continuously. Even today's 'best practice', which is not used to good effect, will not suffice for the development and operation of such systems. The problems of dependably

24 Collins 2004.

25 Collins 2004.

producing large complex distributed systems to match their specifications within time and budget constraints, and the problems of actually achieving adequate operational dependability from such systems when they are deployed, are critical components of ongoing research programmes that will remain important for some time. New means of governance will be essential. Consideration could be given to developing auditing procedures so that large-scale software projects could be certified as having been carried out by appropriately qualified employees, in line with agreed standards.

1.4 Identification and Authentication in Cyberspace

As the automation of business and the use of electronic forms of communications increases, individuals in society are challenged with finding equivalents to such basic security and crime prevention features as face-to-face recognition and hand written signatures. Although the technology is changing rapidly, when two people communicate electronically, for instance, by email, they have usually lost the important facility of face-to-face recognition and need some other means of identifying each other. Similarly, while shoppers in the high street have confidence in the authenticity of the identities of the major stores that they frequent, it is not so easy for Internet shoppers to have confidence in the authenticity of a store's web site.[26]

Identifying People, Devices and Data

Identification and *authentication* in cyberspace involves *primary objects* whether these are people, devices or digital data. The problems associated with identification and authentication in the electronic world need to be considered in the light of the limitations of the techniques used in the pre-electronic age, some of which are highlighted in Box 3.

There are three classic ways for users to authenticate themselves to a system, which may be a computer, network or another individual. They are: (1) something they own, (2) something they know or (3) something they are (i.e. a personal characteristic). Combinations of at least two are common. Typically, the 'something owned' might be some form of token. If that token has some form of processing capability, e.g. a smart card, then the something known might be a password to activate the device. The personal characteristic is likely to be some form of biometric, such as a fingerprint, and this might also be used as an activation process for a smart card. It is now common for a smart card to have encryption capabilities and to contain cryptographic keys. The authentication process may then involve sophisticated protocols between the card and the authenticating device.[27]

Box 3 Authenticating Primary Objects

Suppose, for instance, that you look up someone's telephone number in a directory and dial it. If someone answers and claims to be that person then can you be sure that they are the person you wish to contact? The realistic answer is 'yes, almost certainly'. However, it is worthwhile to stress the assumptions you are making. The first is that your contact is the only person likely to pick up the phone and claim to be them. This, of course, may not be true. Even if the number is correct there may be two people at the same address with identical names, e.g. mother and daughter. The phone call may have been re-routed by a criminal to an impostor who is deliberately impersonating the person you wish to contact. The second assumption is that the number in the directory is accurate. This is almost certainly true if you are relying on a paper version of the directory that has been published by, for instance, the telephone company and it would certainly be difficult for fraudsters to change people's entries. However, the same may not be true if you are relying on an electronic copy of the directory where obtaining assurance that the information has not been altered might be much more difficult.[28]

26 Piper et al. 2004.

27 Piper et al. 2004.

28 Piper et al. 2004.

Before any of these techniques can be used, there must be an identification of the users to ensure that they have, in fact, been given the correct object or knowledge or that the characteristic being associated with them is, in fact, theirs. Most commonly used authentication techniques assume that there has been an initial, accurate identification and rely on that assumption. Authentication techniques that rely on something owned and/or something known cannot authenticate the individual. All that they do is equate the individual with either the knowledge or possession. If the original identification is not conducted properly then obvious disaster looms. Even if the identification process is correct there is always the danger that impostors may either obtain the knowledge or capture the token. In cyberspace it is necessary to prove our identities to one another using a variety of means.

Passwords

The password is the most common form of identification used today. While there are substantial problems with password-based authentication – and these problems mean that passwords are considered a weak form of authentication – it should be noted that passwords are very familiar and convenient and are afforded a wide-degree of acceptability by users. Added to this, administrative safeguards can be used to ensure that user-chosen passwords satisfy certain criteria to help set a minimum level of password acceptability. Users can also be required to change their passwords at regular intervals, and systems often lock-down after a specific number of unsuccessful login attempts.[29]

A particular form of password is the *Personal Identification Number* or *PIN*. We are very familiar with this mechanism from the banking industry, but the PIN is little more than a short, restricted password. The PIN offers very little security, but the PIN is typically used in a two-factor authentication system and it is used in conjunction with the bank (or ATM) card. Fixed passwords have many good attributes –the simplicity and cost of administration – but the risk of password discovery, interception, and/or replay may be too great in some deployments. The *one-time password* is a move towards a stronger means of authentication (see Box 4).

Box 4 One-time Password Schemes

In a one-time password scheme, a user's password is only valid for a short time frame; perhaps for 30 seconds or one minute. After this time the password changes. Thus, the window of opportunity for an attacker is greatly reduced since an intercepted password is unlikely to be of use in the future. All that we require is that the sequence of passwords should not be easy to predict after witnessing or intercepting a (potentially large) set of past passwords.

A one-time password scheme requires a moderate level of computational complexity, and to provide this, the user typically is provided with a token. One of the largest deployments is probably RSA SecurID that can be provided in a variety of forms. The card is issued to a specific user and each card contains a secret quantity, which is also held at the authenticating server. The one-time password is computed as a complex function of the physical time, the unknown secret stored in the card and, optionally, a user-supplied PIN. The password on the token display should then match the password anticipated by the server.[30]

The RSA SecurID[31] technology can be deployed in software and it is supported on a variety of platforms including some mobile phones. In this way, the cost of card deployment is mitigated and the mobile phone can be used as a convenient channel for deployment. Despite the improved

29 Piper et al. 2004.

30 Piper et al. 2004.

31 RSA - Rivest, Shamir, and Adleman.

security offered by the one-time password it is still not classed as strong authentication. Strong authentication requires real-time interaction and the use of cryptographic algorithms.

Encryption

Encryption is the basis for stronger forms of authentication. Instead of transferring a password (or a short-lived password) as a means of authentication, the authenticating server and the claimant (typically a card or token) perform some protocol or exchange of messages. In general terms, the server sends a challenge to the token and a cryptographic computation takes place within the card or token. The result is sent back to the server for verification. The cryptographic computation can be based on *secret (symmetric) key* or *public (asymmetric) key* techniques.[32]

In classical cryptography, the two participants in a cryptographic exchange share the same secret key. Such algorithms are referred to as secret key, or *symmetric*, algorithms. Public key, or *asymmetric*, cryptography allows two participants in a cryptographic exchange to possess different keys. Such systems are designed so that knowledge of one key (the public key) does not allow an adversary to recover the other (the private key). Public key techniques can be used to provide what are termed *digital signatures*. Public key cryptography is not free of problems. In particular, ensuring the availability of authenticated, valid, public keys is a significant problem and one that has proved to be practically tractable in only a few specific areas of deployment. Such a supporting infrastructure is referred to as a *Public Key Infrastructure*, or *PKI*. Cryptographic algorithms are typically classified as shown in Table 1.

Table 1 Cryptographic Algorithm Classification

	Confidentiality	**Authentication**
Secret Key (Symmetric) Cryptography	Block ciphers Stream ciphers	Message authentication Codes
Public Key (Asymmetric) Cryptography	Public key encryption	Digital signatures

Source: Piper et al. 2003.

An alternative to challenge-response protocols based on public key techniques (which are computationally intensive) might be to use what are termed public key based *interactive identification protocols* but these do not provide public key encryption or digital signatures.[33] A summary of the different identification (entity-authentication) mechanisms is shown in Table 2.

People are not the only entity that needs to be identified for cyberspace to be trustworthy. Information in a number of representations (documents, images, sounds, videos), software processes and physical devices (computers, networks, mobile phones, etc.) all have to be identified if a set of trustworthy relationships is to be established between them. At present the main application area is in document authentication, which, in turn, is an important application of cryptographic techniques. In many situations it is the authenticity of information that is far more important than its confidentiality. The term *document* covers the simple electronic representation of physical documents and other forms of digital information such as that carried on a bankcard, executable code downloaded into a device, and virtual and dynamic documents that might contain links to temporary resources on the Internet or might be generated dynamically using temporary data stored on some server.[34]

32 Piper et al. 2004.

33 Piper et al. 2004.

34 Piper et al. 2004.

Table 2 Entity Authentication Mechanisms – Pros and Cons

Technique	Pros	Cons
Fixed passwords	Familiar	Vulnerable to simple dictionary attacks, interception and replay. Closed-system deployment.
	Simple to use	
	Simple administration.	
One-time passwords	Simple to use	Typically needs a hardware-token together with supporting infrastructure. Closed-system deployment.
	Relatively simple administration.	
	Less vulnerable to replay attacks.	
Challenge-response (secret key)	Simple to use	Typically needs a hardware-token together with supporting infrastructure. More complicated interaction than for one-time passwords. Closed-system deployment.
	Relatively simple administration	
	Cryptographically strong	
Challenge-response (public key)	Simple to use	Typically needs hardware token together with supporting infrastructure. Administration can be involved and protocols can be computationally intensive.
	Cryptographically strong.	
	Open-system deployment possible.	
Identification protocols	Simple to use	Typically needs hardware token together with supporting infrastructure. Administration can be involved. Less cryptographically versatile than public-key challenge-response.
	Cryptographically strong	
	Open-system deployment possible.	
	Computationally cheaper than public-key challenge-response.	

Source: Piper et al. 2003.

People are not the only entity that needs to be identified for cyberspace to be trustworthy. Information in a number of representations (documents, images, sounds, videos), software processes and physical devices (computers, networks, mobile phones, etc.) all have to be identified if a set of trustworthy relationships is to be established between them. At present the main application area is in document authentication, which, in turn, is an important application of cryptographic techniques. In many situations it is the authenticity of information that is far more important than its confidentiality. The term *document* covers the simple electronic representation of physical documents and other forms of digital information such as that carried on a bankcard, executable code downloaded into a device, and virtual and dynamic documents that might contain links to temporary resources on the Internet or might be generated dynamically using temporary data stored on some server.[35]

When considering the authentication of a document the complexity of the document can have a significant impact. When we sign a stand-alone electronic document, or some executable code, then it is (reasonably) obvious what we intend the signature to cover and what we intend the signature to mean. However, if a document were to contain links to, or be generated by, other temporary resources, then while the implication behind the signature might be obvious, its execution and continued validity can introduce some significant problems.

35 Piper et al. 2004.

How to extend the concept of identity into these complex areas and engineer reliable solutions are as yet poorly understood.

Biometrics

The only authentication techniques that attempt to authenticate a user *directly* are biometrics. The term biometrics is derived from the Greek words bio (life) and metric (to measure). The field of *biometrics* is the measurement and statistical analysis of biological data. Biometric authentication methods cannot be passed on to others and losing them is difficult (and even if the feature is 'lost', it cannot be used by somebody else). However, the possibility of impersonation by forgery may be possible.[36]

In a biometric system a personal characteristic such as a fingerprint is used and the basic assumption of the authentication process is that a person's fingerprint identifies them uniquely or, more accurately, that the probability of two people having identical fingerprints is so small that it can be safely assumed to be zero. In a typical biometrics system, a user will give a number of copies of the chosen biometric which are converted into bit patterns and stored on a template. When that user wishes to authenticate to the system he or she provides a copy of the chosen biometric and that copy is compared to the template. If the copy provided is 'close enough' to the template then the user is authenticated. A fundamental problem with applying biometrics is the determination of what is acceptable as 'close enough'. The main biometric methods in use today are: fingerprint recognition, hand geometry reading, iris scan, retinal scan, face recognition, signature dynamics, and speaker recognition.[37]

Table 3 General Requirements for Biometric Methods

Requirement	Description
Universality	Each person should have the characteristic.
Uniqueness	No two persons should have the same characteristic.
Permanence	The characteristic should neither change nor be altered.
Collectability	The characteristic can be measured quantitatively.
Performance	The characteristic can be efficiently measured in terms of accuracy, speed, robustness, and resource requirements.
Acceptability	The characteristic should be acceptable to the public.
Circumvention	There should be no easy way to fool the system.

Source: Piper et al. 2003.

In order to be applicable for authentication, a biometric method must fulfil the general requirements shown in Table 3. No current technology is available or will become available that meets all the requirements to the fullest extent because those who seek means of circumvention will continue to do so.

Before a biometric system can be used, the user (identified in some way) has to *enrol*, providing the system with his/her biometric reference data which are stored and used to produce a template which is matched with one (in the case of verification) or many (in the case of identification)

36 Piper et al. 2004.

37 Piper et al. 2004.

reference templates. No two biometric templates match 100 per cent and their similarity has to be calculated. In order to make a decision, a certain threshold is defined which maximises the acceptance rate for authorised users and minimises the acceptance rate for impostors. Two types of error are defined to measure the performance of biometric systems.[38]

> Type 1: The system fails to recognise a valid user (*false rejections*).
> Type 2: The system accepts an impostor (*false acceptance*).

While there is not necessarily a precise link between the two error rates, in practice they are typically linked. When the false rejection rate is kept small, the false acceptance rate tends to rise, and vice versa.

The application domains for biometric authentication coincide with the applications domains of conventional authentication methods, namely access control to networks, physical access control to sites, entity identification and time and attendance control among many others.[40] Some applications that have attracted attention in the media include passports and identity cards. Many airports now issue smart cards with biometric templates to allow speedy checks at immigration. In the US the biometric is typically either hand geometry or a fingerprint, while at Heathrow Airport in the UK it is iris recognition.[41]

The Usability of Authentication Mechanisms

Cyberspace is enabling new forms of attack on people and their possessions and the declining cost of technology makes cyberspace attacks less risky for the attackers. Changes in the design of secure technologies and in social practices and cultural norms of information assurance influence whether strategies to reduce criminal acts or threats arising from unintended changes in information handling procedures will be effective.

Although there are many mechanisms for authentication, there is no single mechanism for usable authentication. This is because the answer to the question 'which is the most usable authentication mechanism?' is that it depends on the characteristics of the user group, the task, and the physical and social context in which users and security mechanisms interact.[42] In addition, the available mechanisms may be hard to use or ineffective because they make unreasonable demands on their users.[43] Box 5 summarises research on the usability of alternative means of authentication.

38 Piper et al. 2004.

39 Piper et al. 2004.

40 Woodward et al. 2002.

41 Piper et al. 2004.

42 Schneier 2000, 2003.

43 Checkland 1999; Sasse 2003; Zurko and Simon 1996.

Box 5 The Usability of Authentication Mechanisms

The functioning of human memory makes strong passwords difficult to use. Users report that they have an increasing number of passwords to remember and regularly encounter problems with infrequently used passwords.[44] In one study, 52 per cent of failed logins were due to users who entered the wrong password.[45] Research on human memory has established that human performance at recognition is far superior to unaided recall, and images are processed and stored differently from words, and easier to recall.[46] Graphical passwords authenticate users through recognition of images, or features of images. Studies suggest that these perform better than passwords and other forms of infrequently used authentication,[47] but informal reports from commercial trials indicate that this performance advantage disappears rapidly when users have multiple logins using the same type of image or the images/faces are changed, and they can be very slow.[48]

Knowledge-based authentication in the form of passwords and PINs creates unacceptably high costs for users and organisations in terms of stress, low task performance due to failed log ins, and reduced productivity.[49]

Tokens have been used, with apparent success, for remote access by financial institutions, but the high cost of replacing lost tokens and/or lost working time has led companies in other sectors to abandon it. Users may need a collection of tokens, which they will find hard to manage, but a single token carrying multiple credentials raises issues for privacy protection.[50]

Biometrics are not secret and they can be harvested from legitimate users and systems which then can be attacked.[51] Some users are temporarily or permanently unable to register a particular biometric; five per cent of people are estimated not to have readable fingerprints and blind users cannot register iris images. Temporary inability to register or use a biometric can result from cuts or burns on fingers for fingerprints, or pregnancy or certain types of medication for iris recognition.[52] Biometric authentication raises the question of acceptability among some user groups for religious reasons, because of safety and privacy concerns, and as a result of labour relations concerns about monitoring employees.[53] Many banks in the UK and Germany have ruled out use of biometrics on cash dispensers in the foreseeable future, because of concerns about how customers will respond to false rejection and because the cost of the technology is too high.[54]

The usability of any authentication mechanism depends crucially on the nature of the task to be performed. A well-designed mechanism needs to maximise the effectiveness and efficiency of task execution.[55] Failure to provide users with the necessary understanding, training and motivation will cause human error.[56] Users are often left to make a choice between complying with security regulations and completing a task.

---

44 Adams and Sasse, 1999; Sasse et al. 2001.

45 Brostoff and Sasse 2000, and see Dhamija and Perrig 2000; Petrie 2002; Yan et al. 2000; Yan 2001.

46 Schacter 2002.

47 Dhamija and Perrig, 2000; Valentine, 1999a,b.

48 Brostoff and Sasse, 2000.

49 Adams and Sasse, 1999.

50 Torinofacile, 2003.

51 Schneier, 2000; 2003.

52 Fairhurst and Deravi, 2001.

53 BIOVISION, 2003; Coventry et al., 2003.

54 Sasse 2004; see also Frith and Blakemore 2003; McClue 2003; Morris et al. 2003; Thiel, 2001; and O'Hara et al. 2003 for Foresight research on memory and cognition.

55 Sasse 2004.

56 Reason 1990.

The selection of a security mechanism and how it is configured should not be left to security experts because their usability depends on the context of business processes and workflow.[57] Empirical studies of users of ICT systems suggest that many users are not motivated to comply with security regulations because they do not believe they are personally at risk or that they will be held accountable.[58]

Cyber-security and Risk Management

Empirical research has examined the conditions under which end-users of cyberspace systems might begin to offer solutions to many cyberspace security problems.[59] Studies show that if a 'culture of security' can be fostered, end-users may take on the responsibility for monitoring risks and taking appropriate action.[60]

The case study in Box 6 indicates the importance of appreciating the many subjective understandings of risk and the importance of communicating risks effectively by considering the medium as well as the message.

Box 6 Security and Risk Communication

A case study of an effort to launch an Internet banking product in a top-tier global bank – NIMETBANK - indicates that individuals and institutions process messages they receive and develop their perceptions of messages according to previous experiences, the social and economic climate, their cultural backgrounds and the trust they place in messages and their sources.[61] Trust was placed in the technologists who had delivered in the past. In order for us to trust a message, we need first to trust the communicator. Credibility of information sources is a key factor in risk communication such that credible sources are those who shape risk and security policies within organisations.[62]

Internal control systems are crucial to system security as demonstrated in the case described in Box 7 where issues of control in decentralised organisations are depicted to show the difficulties of establishing operational norms among different cultures and sub-cultures.

57 Brostoff and Sasse 2001.

58 Weirich and Sasse 2001.

59 Backhouse et al. 2004.

60 Parker 1997; Osborne 1998; von Solms 2001 Wood 1995.

61 Bener 2000; Backhouse et al. 2004.

62 Backhouse et al. 2004; Fesseden-Raden and Fitchen 1987; Krimsky and Plough 1988.

Box 7 Interpreting Security Control Rules

The relationship between formal systems and informal organisational norms has been investigated in a global bank with branches in London and Bangkok.[63] A relatively flat matrix management system led to security guidelines being ignored in the local branch in Thailand partly because of the absence of a designated bank manager in the branch and the London manager's failure to be responsive to the different cultural context in Thailand. Hofstede identifies dimensions of the cultural contexts that give rise to 'social risk'.[64] In the Thai branch the status of the formal rules was undermined by organisational changes and staff were resorting to personal judgments. The key lesson is that global policies and standardised manuals and procedures of multinational firms are not internalised in the same way in every branch, as anticipated by the management of this bank.[65]

As corporate experience with the use of Public Key Infrastructure shows (see Box 8), the technical capacity to interoperate must exist alongside the interoperability of institutions and their policies and practices. One instance of this is particularly evident in the case of standardised directories.

Box 8 Security, ICT System Interoperability and Identity Management

Standardised directories may be used to avoid interoperability problems where digital certificates and a Public Key Infrastructure (PKI) are in use.[66] A case study examined two global companies in the oil and finance sectors to show why it is so difficult to implement technical standards.[67] The success of PKI in Oilcom was attributed to a campaign to knit it into the organisation, but 'islands' of PKI began to emerge for Oilcom's outward-facing trust services. At Bankrecht PKI was less successful because of the absence of widely accepted institutional order and this led to the proliferation of PKI 'islands'. Both companies were depending on 'circles of trust' in closed trade bodies, rather than on the PKI model's capacity to verify identities.[68]

In the light of growing evidence of the importance of behavioural factors in achieving ICT system security, there is a shift in security management from concern about technical devices to management issues. This is evidenced by the success of codes of information security management developed in the UK (BS7799) and by the International Organisation for Standardisation (IS017799). The next phase of security management is likely to focus on the interoperation of management policy for a number of business processes such as document sharing, collaborative working and on-line dispute resolution, giving rise to the need for new theoretical frameworks that can be applied to address these issues. At an organisational level, the most immediate change to achieve a 'culture of security' is to integrate security into business processes.[69] Once security aims appropriate to the organisation are established, role models are essential to change behaviour and re-build the security culture to make secure behaviour a desirable trait that becomes part of professional and ethical norms.[70] In addition, ratings service

63 Chauvidul 2003.

64 Hofstede 1991.

65 Backhouse 2003.

66 Chokhani and Ford 2003; Ellison 1997.

67 Clegg 1989; Wamala 2002.

68 Backhouse 2003.

69 For empirical data on high-tech crime in the UK see National Hi-Tech Crime Unit (2004).which indicates that of a sample of 105 business employees the following computer-related crimes were identified as serious – sabotage of data or networks 91%; virus attacks 90%; financial fraud 88%; theft of proprietary information 86%; attacks, e.g. Denial of Service 79%; theft of laptops 76%; unauthorised website access/misue 75%; spoofing attacks 74%; theft of other hardware 71%; telecommunications fraud 55%; telecoms eavesdropping 48%; and active wiretapping 43%.

70 Sasse et al., 2001; Sasse and Brostoff, 2001.

providers such as Standard and Poor's and Moody's are likely to begin offering operational risk ratings for cyberspace services in the future.[71]

Future Prospects for Trustworthy Cyberspace

Weaknesses in currently used methods of ICT system development and in identification and authentication mechanisms allow exploitation by criminals. Most solutions are appropriate for certain environments and inappropriate for others. There is progress in securing different aspects of the cyberspace infrastructure, but the issues are complex and, as yet, not well formulated.

Persuasive design techniques offer a means for designing systems that intrigue and, thereby, persuade and reward users for good security behaviour.[72] Developing usable security mechanisms is not simply an issue of 'fixing' user interfaces to current mechanisms. Appropriate and effective security must be an integral part of the socio-technical system it is supposed to protect. Effective security must take into account the needs and potential conflicts of all stakeholders.[73]

Security needs to be integrated into ICT development approaches. It should be part of the software engineering documentation that developers work with. Technical design decisions must consider the mental and physical workloads imposed on system administrators as well as end users. Despite the fact that different authentication methods are frequently adequate for their purpose, they display obvious security limitations. Tokens can be lost or stolen and passwords and PINs can be guessed or copied. The use of biometrics can, at least in theory, remove some of these insecurities. We have reached the situation where some biometric authentication techniques have become quite advanced, but it is not clear that there is yet any reliable consistency in biometric products.[74]

System integration is essential even in the case of the use of biometrics because the transmission of biometric data between different system components is one of the main weaknesses of a biometric system. Biometric data are transmitted from the sensor to the feature extractor and then to the matching module and onto the application. There is also a need for alternatives for users who inadvertently fail or are unable to use a given biometric test. The best solution might be to have the reference data (templates) stored on a smart card or another device that the user can carry.

Matsumoto used sweets called *gummy fingers* to create forged fingerprints and this highlighted the future importance of *liveness detection*, i.e. the biometric template used at both user registration and authentication should be from a live user.[75] In the future, secondary levels of authenticity and trustworthiness will become very important as will methods of controlling information and metadata.[76] As compared to issues of primary object identification and authentication discussed above, issues of secondary authenticity are more subtle and complex.

Secondary authenticity and trustworthiness

When we authenticate (or identify) a human or a computational device we often make the assumption that the supporting infrastructure will be trustworthy and that it will behave as intended.

---

71 Backhouse et al. 2004.

72 Fogg 2003.

73 Friedman et al. 2002; Sasse 2004; Seymour Powell 2000; Whitten and Tygar 1999.

74 Piper et al. 2004.

75 Matsumoto 2002.

76 Piper et al. 2004.

Without this assumption it is difficult to imagine that any solutions will be viable and there is a tendency to acknowledge and then ignore this issue.[77] All the security mechanisms discussed above could be compromised easily by a simple failure in the administration procedure. Many security problems occur when the human being directly interfaces with the digital world. This happens at user registration and when a user is prompted for action by some application. It requires a leap of faith to assume that the whole system will work as intended. As more rights are managed and conferred by digital means – for instance with the use of digital identification cards as a way of providing access to services – the stakes are raised and the illicit gains of fraudulent behaviour are likely to increase. Box 9 highlights a few of the issues in this area.

All these developments raise issues for the control of information and metadata in cyberspace.

Box 9 Safeguarding the Trustworthiness of Infrastructure

Consumer devices – Personal computers, Personal Digital Assistants (PDAs), and mobile phones can import code that changes their functionality. To help decide between good and potentially malicious code, initiatives such as code-signing are developing that allow a device to digitally verify the authenticity of a particular application.

Smart card manufacturers spend millions on the best ways to provide additional security features on the cards they produce. The integrity of a smart-card based solution is dependent on the fact that the smart card offers a secure storage and computation environment.

Secure computing initiatives such as Palladium and Trusted Computing Platform Alliance (TCPA) provide a secure and trusted computing environment.

Good engineering and secure coding practices are being promoted, but it is unclear whether good security implementation practices are being used within deployments.[78]

Controlling Information and Metadata

Controlling information is fast becoming the issue of our times. Pervasive computing and *ad hoc* networking are giving rise to the need to authenticate *dynamic documents* that either point to transitory information or use transitory information in their construction.[79] *Meta-data* are *information* that has attached to it additional information serving as a description of its use and functionality. An extension of this concern occupies the minds of executives at companies providing entertainment content, e.g. music and videos. The use and potential misuse of this information drives the whole area of *Digital Rights Management* (DRM) and leads us full circle to the issue of registration of identity or ownership. One DRM solution that is much discussed is effectively to 'register' the devices on which information can be accessed. Unlike the case of human registration where there is no digital interface, registering a device is technically straightforward (despite the formidable privacy and consumer-acceptance issues involved).

In the future, the concept of *ICT system trustworthiness* will need to be broadened to include *reliability*. Catastrophic system failures are usually fairly easy to detect and, more often than not, to fix. Intermittent problems that lead to degradation rather than to outright service failure are harder to address. For this reason it will be very important to address the continued robustness or dependability of the supporting cyberspace infrastructure. As agent software is used for workflow,

77 Piper et al. 2004.

78 Piper et al. 2004.

79 Piper et al. 2004.

middleware and automatic negotiation, the importance of identification and authentication of software and data objects, as well as people, will grow.

Original identification is also likely to become an issue in the future as suggested in Box 10. Consideration will need to be given to people's attitudes to intrusive measures such as taking DNA samples at birth or inserting chips. The likely physical consequences of implanting chips in a person's body for life and the durability of the chip will need to be examined. As the example of John and Mary Smith suggests, the general problem of identifying 'the original' is a difficult one and one that is frequently overlooked.

Box 10 The Problem of Original Identification

Suppose that we are confident that we know the identity of Mrs. Mary Smith. If her son wanted his identity to be John Smith, son of Mrs. Mary Smith, and for this relationship to be authenticated, then there is only one stage of his life at which we can have total confidence in this claim. That is, while the umbilical cord is still joining John to his Mother, Mary.

As soon as the cord is cut, procedures are required to ensure that there is some form of binding between John, his identity and the relationship with his mother. If these procedures go wrong, for whatever reason, then either someone else will have John's identity or John will have the wrong identity, or both. If we wish to be confident that John Smith has the correct identity and authenticated relationship with another human being, his mother, for the rest of his life, it could be argued that the binding must take place while the umbilical cord still provides an undeniable physical link between the two parties. Two obvious options that are often discussed are: taking a DNA sample or the physical insertion of a microchip containing the baby's identity into the body. If the DNA sample is taken then procedures are still needed to ensure that the record that associates the DNA sample with John Smith is accurate and cannot be altered at any time during John's lifetime. If the chip is inserted into John's body then there need to be assurances that this cannot be removed or replaced by another person and that the information stored on the chip cannot later be changed via remote access.

If such procedures have not been followed, then it is necessary to rely on robust procedures to ensure that there is a means of auditing the provenance of the respective samples and the testing and reporting procedures.[80]

The problems associated with establishing identity are frequently ignored in discussions relating to the issuance of passports, digital certificates and all the authentication techniques that rely on biometrics. Most of the current methods of establishing identity seem to depend on the fact that that person's identity has already been established somewhere else. Each new process is merely endorsing the old one. There are numerous examples of where the ability to impersonate someone at some point in the registration stage implies the ability to steal his or her identity and impersonate the person for life.

ICT Forensics in the Future

ICT Forensics as a branch of Forensic Science is in its infancy. The practice is mainly involved with data held on hard disks in PCs, PDAs and other flash memory devices. These are used by criminals for some activity and, when captured, the data on the devices provides evidence of malfeasance. In order to provide such evidence, all entities (documents, computers, disks, etc.) concerned with the case have to be identified and authenticated. People are identified using traditional techniques and their use of systems is authenticated via system logs.

The strength of the process of authentication of all entities that are considered valuable to detecting, investigating and prosecuting crime is critical in the case of digital evidence. If a digital

80 Piper et al. 2004.

image is produced as evidence it needs to be protected from alteration. Furthermore, if the digital image is obtained using a digital camera then it is necessary to verify whether it is the original. If the protection, such as a digital signature, is constructed and attached inside the camera then we need assurances about the tamper-resistance of the camera. If it is applied using another device then we need procedures to ensure that it was not changed before the protection was applied.[81]

The general problem of identifying 'the original' for authentication purposes is difficult and frequently overlooked. This topic has a direct bearing on the trustworthiness of cyberspace and our ability to successfully prosecute crime where digital evidence is used. Similarly, if a document, i.e. an e-mail, a transcription of a phone call or an internal memo, is seen to provide evidence of a criminal activity, then some 'proof' that a certain person authored the original and when and on what 'machine' they did that is essential if the document is to stand up in court as evidence. The quality of the proof will rely on not only the raw data and metadata, but also on the veracity and traceability of the process by which these data and metadata are managed between the time they are obtained by the law enforcement agency and by the court.[82]

For the future, however, a number of developments are seen as being either disruptive to current processes or scaling up the problem to such an extent that new ways of dealing with computer forensic investigations will be essential.

Key issues are likely to include:

Scale of systems: the volumes needing to be searched in order to find data that might be of interest to a law enforcement agency are growing exponentially. Obtaining specific information to reduce this volume will become more and more problematic as distributed storage, possibly incorporated in a grid architecture, becomes the norm. However, legitimate users will face the same problem. Tools that deal with such scale will be developed, but they may not have the processes of auditability and traceability incorporated in them that will be necessary for evidence gathering unless this is laid down as a requirement at the outset.

Distribution of data: data will, all other things being equal, be stored wherever it is most efficient to store them; this may not be in the jurisdiction of the law enforcement agency which needs to investigate an alleged crime or gather evidence for one that has certainly occurred. Unless some form of international code of practice, perhaps under the umbrella of newly agreed digital principles (section 7.7), is agreed. It will become increasingly difficult for law enforcement agencies to access data to detect crimes and prosecute criminals.

Lack of strong binding between data and suspect: as the world of electronic commerce and other electronic services spreads geographically and becomes much more pervasive, ensuring the ability to connect the record of any action with an information object such as a document, video or audio record will become more and more complex and potentially expensive. In order to prove in court that there is a connection between an information object and a person, both must be identified *and* a link between them established with appropriate spatial and temporal proofs. The strength of the evidence of this link, usually referred to as the strength of the binding mechanism, will become critical in establishing the proof that will be needed in court. A more relaxed objective could be to establish sufficient strength to allow other physical investigations to be instigated under warrant to gather stronger evidence. In both cases, collaboration between system designers and legal and law enforcement specialists would greatly increase the probability that this issue does not become a major obstacle to crime detection.

---

81 Piper et al. 2004.

82 Current advice on the management of computer crime-related evidence is contained in the ACPO (Association of Chief Police Officers) guidelines which can be found at http://www.nhtcu.org/ACPO%20Guide%20v3.0.pdf accessed 11 Feb 04.

Mass storage devices: the availability of mobile and transportable miniature mass storage devices will expand enormously over the next decade. The current use of devices, such as i-Pods for music storage, will expand to encompass video and data. From a crime prevention viewpoint these devices have a number of undesirable properties; they store huge volumes of data which can be protected at the document and device level using strong encryption-based authentication, are only connected to a system when plugged in or connected via a wireless network, and can be very easily concealed and, in extremis, destroyed. Reliance on the analysis of log files to identify when and where specific devices have accessed or are accessing systems and networks and being able to very rapidly and accurately trace subsequent use seems the only opening at present for tracing illegal activities being perpetrated through the use of such devices. This is an extension of what is now possible for mobile telephony but on a much greater scale, with concomitant expense; the question of whether the public or private sector wishes to bear the costs of very expensive tracking or endure rapidly spreading un-prosecutable crime could be an urgent subjects for debate.

High quality encryption: high quality encryption has been freely available for decades. Little visible use is being made of it as yet by criminals, but most experts in the field consider it is only a matter of time until this happens. If and when it does, another layer of complexity in detection and prosecution will emerge, especially if there is widespread use of encryption for privacy or commercial-value protection. This will cause there to be a greater volume of encrypted material within which the criminal can conceal his or her activities. One mitigating circumstance is that if data can be shown to be encrypted and not legitimate, they could be used to make a case for further investigations under warrant. This would also have to be widely in line with new principles and practices (section 7.7).

Gap between user system developments and forensic tools: forensic tools are developed by a very small number of academic groups and companies to meet the specific needs of current case work. User system development attracts billions in development investment to provide highly sophisticated user functionality in products such as SAP, MS Office, Oracle and bespoke systems for banks, trading floors, on-line news services and air traffic control. It is inevitable that without some collaboration with such developments, the ability of investigators and computer forensic experts to maintain parity with the environment within which the data under investigation are used and stored will be limited. Such collaboration until very recently has been sporadic. Unless the ability to carry out forensic investigations is seen as being a legitimate requirement of a system or application design, this situation is likely to get worse, and the ability to prosecute e-crime using computer forensics could become largely non-existent.

Inertia in legal systems: the rate of change in society as a result of the spread of the Internet is probably unprecedented in recent centuries. Legal institutions and procedures are perceived by some to have changed very little as a result of the growing use of on-line services. This may be unfair criticism, but the gap between fact and perception is an important social phenomena. The creation of a forum in which dialogue could occur to clarify this situation would be highly beneficial to all concerned. However, for such a forum to be trusted, the fundamental issue is how various stakeholders might react to legal initiatives and ethical discussions, and hence which type of organisation (government, judiciary, parliament, society, commerce, learned society) should initiate it.

The nature of computer forensics: computer forensics, at present, is largely an activity in support of evidence-gathering by law enforcement agencies. A certain amount of support is given to investigative work but very little to preventative investigations. Why this is the case is unclear. Candidate reasons are too few experts, rapidly changing systems, lack of access to suitable environments or hesitancy by owners of systems as to whether they ‘want to know’ in advance of any potential weaknesses. The negative reaction to the Y2K preventative investment after the perceived ‘non-event’ is indicative of that attitude may be the dominant cause. However, it is clear

from the after the Y2K programmes that considerable improvements were made in system resilience as a result of the preventative work carried out. Hence, consideration could be given to what balance could be struck between evidential - investigative – preventative computer forensics and the risks and benefits of options.

Current research: research centres around applied activities that are derived from ongoing case work. Tools and techniques are being developed in an attempt to place the law enforcement agency and the investigator in a good position to 'do better next time' when another case arrives. There would appear to be little fundamental work being carried out, especially dealing with the difficult problems outlined above with respect to scale, complexity, criminal strategy, legal and constitutional issues, and the impact of new technologies.

1.5 Lessons for Cyberspace Dependability and Security

A survey carried out by UK Department of Trade and Industry and PricewaterhouseCoopers in April 2004[83] indicated a rapidly growing dependency in British industry and commerce on critical information held in computer systems and an increase in the use of the Internet and the web in business in general. These factors combined to show an increase in security incidents of all types even though there was heightened awareness of the need for good security. This survey indicated the need for improvements across the board if business were to maintain or improve the dependability of services derived from the use of such systems.

Dependable pervasive systems will be constructed out of multiple pre-existing systems and will also need to be highly adaptable. Most will embody human beings as system 'components'. The successful design and deployment of such systems is a major challenge that calls for socio-technical as well as technical dependability expertise. Cross-disciplinary approaches to research and to operation are essential if any inroads are to be made in this field.

Once designed and implemented, pervasive computing systems must incorporate means of identifying users and of authenticating that users are who they claim to be for many purposes and applications in cyberspace. This is giving rise to the need for both human and technical measures to secure cyberspace that are responsive to the needs and behaviours of the users. We have examined a number of identification and authentication techniques. If they are to be trusted then the process of *original identification* must be adequate. Technical research into the security of technology is needed together with research on the effectiveness of the identification processes used for important everyday processes such as passport applications, bank account/credit card applications, including their costs and failure rates.[84]

Encryption is, at present, the only 'strong' mechanism available and it is now in reasonably widespread use. However, there are situations where it can be subverted or used as a tool for denial of service. An outstanding question is - how much 'security' or 'strength' is appropriate? Procedural approaches and architectural solutions (separation of duties) can be used to significantly reduce the risk of vulnerabilities arising as a result of human behaviour in what might otherwise be 'trustworthy' processes.

Education programmes could be used to highlight the need for compliance with local security policies by drawing attention to the relationships between offenders, targets and guardianship relationships using a systematic framework linking risk, information system security, audit,

---

83 See http://www.pwc.com/Extweb/service.nsf/docid/B2ECC9B0E9EFA3D785256C33005247D3 accessed 6 May 04.

84 Piper et al. 2004.

compliance, and human relationships. This would avoid the tendency for security systems to be developed in isolated ‘silos’ within organisations.

This section shows that: 1) developments in pervasive computing involve important organisational and human behavioural issues; 2) assumptions about the work organisation of software engineering teams and collaborations between developers, and between developers and end-users need to be examined; and 3) solutions for user identification and authentication depend on their usability and their security, neither of which can be addressed only through technical means.

4 EXPERIENCING TRUST AND RISK IN CYBERSPACE

Many assumptions about trust and risk in cyberspace are made by cyberspace technology developers and users. These assumptions are examined in this section to suggest why there are divergent views about person-to-person, person-to-system, and system-to-system trust in cyberspace and the implications for crime prevention.

The trustworthiness of the 'space' implemented by the use of pervasive ICTs will only be enhanced when we have a deeper understanding of how knowledge, the currency of the knowledge society and the economy, can be managed throughout its whole life cycle, by both people and agents, and interactively and collaboratively, in such a way that outcomes of transactions and interactions are predictable, at least generically, and are perceived as being reasonably safe. To achieve this, it will be necessary for the barriers to criminal or socially unacceptable use of ICTs to be sufficiently high to minimise opportunities for unpredictable interactions associated with behaviours that are not socially valued. The way system components interact dynamically to add value to society and the way critical technologies support social processes that may lead to cyberspace crime prevention both need to be understood from a variety of perspectives.

We can draw on research focusing on risk perception and on trust and the nature of trustworthy systems to understand the relationships between risk appraisal, the likelihood of forging trusted relationships in cyberspace, and the development of norms and practices that are consistent with crime prevention. The extent to which people are likely to accept government intervention or controls over their behaviour in cyberspace depends upon whether they are informed about the potential risks of cyberspace and whether they perceive themselves to be at risk. It is unclear whether the technical possibility of risk in cyberspace is the same as the reality of the perception and experience of risk. We are in the early stages of creating an evidence base to assess whether people act according to their perceptions of risk or their experience of actual incidents in cyberspace. These factors influence people's willingness to place their trust in cyberspace. As in other areas of technological innovation, cyberspace is being developed in an environment that Beck and Giddens have called the 'risk society'.[85]

1.6 Public Perceptions of Risk – Appraising Uncertainty

Research on public perceptions of risk suggests that the social meaning of a risk influences its salience and how uncertainty is judged. Concerns about risk express underlying values and attitudes to blame, morality and the value placed on the outcome of an event. Public opinion is often contrasted with expert assessments of risk and this is particularly so in the case of crime that is facilitated by cyberspace.[86] Disputes about differing conceptions of risk cannot be settled by stipulating definitions for disputed terms because they are systematically linked to 'probabilistic' and 'contextualist' dimensions of risk (see Box 11).

Box 11 Probabilistic and Contextualist Dimensions of Risk

The probabilistic view of risk suggests that risk is purely a matter of the probability of an event or its consequences. From a contextualist perspective, risk has no single determining criterion. A risk will always be associated with a number of characteristics. Probability, in this view, is simply one among other risk attributes. From the strong contextualist perspective, probability estimation may be irrelevant to determining the existence of a risk or for communicating it to others.[87]

---

[85] Beck 1992; Giddens 1991.

86 Jackson 2003; Lieratore 2000; Ravetz 1987.

87 Jackson et al. 2004; Thompson 1999; Thompson and Dean 1996.

The way the public sees experts and regulators may influence how risks, such as those perceived or actually experienced in cyberspace, are interpreted. The relative failure of risk communication strategies in relation to technological risks, has given rise to substantial research on the role of trust in risk perception.[88] Public anxieties in the UK about GM food, BSE, rail safety, mobile phone transmitter masts and a host of other risks may be explained by a lack of trust or confidence in those responsible and a loss of legitimacy of certain public institutions.[89] However, as O'Neill suggests, it is important to distinguish between perceptions of trust as reported by participants in empirical studies or in the media and the 'practical demands of placing trust'.[90] She argues that the relationship between perceptions of trust and trustworthiness and placing trust in public institutions, scientific evidence or professional judgement is not straightforward.

> 'The connection is that those who see their world as a "risk society" often find placing trust problematic: but it does not follow that they do not place trust, or even that they place no trust in those whom they claim to think untrustworthy'.[91]

This perspective is important when we consider some of the insights from empirical studies in the field of trust and risk perception that are highlighted in Box 12.

Box 12 Empirical Studies of Trust in Risk Perception

Empirical research on the role of trust in risk perception includes work by Freudenburg (1993) on the effect of trust on the concerns of local citizens and by Slovic on the asymmetrical effects of trust building and trust destroying information. Slovic showed that the effect of negative information on trust 'destruction' is much greater than positive information on 'trust building'.[92] Trust is related to beliefs and expectations that some possibly remote institution or actor will act in a particular way in a particular context.[93] A lack of trust that leads people to see risks as greater may be based on expectations about risk managers' competencies. Rather than deducing trustworthiness from direct evidence, people infer it from 'value-bearing narratives' using information shortcuts and images.[94] Trust may be higher when the narratives or stories told by institutions express salient values that are similar to their own.[95]

Douglas argues that beliefs about purity, danger and taboo are essentially arbitrary. Once they become fixed, they serve to organise and reinforce social relations according to hierarchies of power.[96] An individual's beliefs about what constitutes an important risk are also indicative of his or her place in society.[97] This observation shifts the emphasis away from individual differences or biases in perception of objective risks towards the role of inter-group distinctions. People's conception of what constitutes danger, or a risk, may vary according to the way their social relations are organised. People may select risks as being important or trivial because this

88 Cvetkovich and Lofstedt 1999.

89 Douglas 1966; Douglas and Wildavsky 1982; Poortinga and Pidgeon 2003; Rayner 1992; Thompson and Dean 1996.

90 O'Neil 2002.

91 O'Neilll 2002, p. 12.

92 Slovic 1993.

93 Barber 1983; Luhmann 1979.

94 Earle and Cvetkovitch 1995; Siegrist et al. 2000.

95 Jackson et al. 2004.

96 Douglas 1996.

97 Rayner 1992.

reinforces established social relations within their culture, although they may revise their thinking over time.[98]

Insights into the perception of risk and trust can be drawn from theories in cognitive psychology, psychometric research, and studies of the relationship between emotion and risk perception (see Box 13).

These insights need to be examined in the light of people's perceptions about the riskiness of cyberspace, which remains an under-researched area. Their perceptions are likely to be influenced by the signs, symbols and representations they encounter within their social networks and through the media's reporting of cyberspace events. Social meaning must be expected to influence appraisals of a perceived threat or an uncertain event in cyberspace and it places risk objects within a cultural context.

Box 13 Contributions from Psychology

Cognitive Psychology

Risk perception can be seen as a matter of judgement about an uncertain event – its likelihood and its consequences. People do not follow the principles of probability theory when judging the likelihood of uncertain events. They employ 'rules of thumb' and Prospect Theory suggests these include the representativeness of an event and the ease of recalling a similar class of events. The greater the ease of recall, the more numerous such events are likely to seem.[99]

The Psychometric Paradigm and Risk

The psychometric approach to the study of risk perception[100] has helped 'to demonstrate that the public's viewpoint must be considered not as error but as an essential datum'.[101] This approach aims to elicit judgements about risks from individuals who are confronted by hazard stimuli in order to understand quantitative judgements about risks and the subjective dimensions.[102] Personal risk taking activities are seen as less risky and more acceptable.

Emotion and Risk Perception

A distinction is drawn between two modes of information processing: formal, logical and numeric reasoning and 'intuitive, automatic, natural, non-verbal, narrative, and experiential' reasoning.[103] This approach highlights the interplay between emotion and cognition.[104] A stimulus can evoke images that become tagged with affect, such that the overall affective impression can be more influential than more cognitive assessments. This may increase judgements of riskiness and decrease the perceived level of benefit.[105]

Murdock et al. suggest that the media can amplify or attenuate perceptions of risk if they resonate with public feelings and mood and if the symbols and representations capture existing public concerns and frames of reference.[106] Petts et al. show how patterns of talk and the structures of

98 Jackson et al. 2004.

99 Kahneman et al. 1982; Kahneman and Tversky 1979.

100 Slovic et al. 1979; Starr 1969.

101 Royal Society for the Prevention of Accidents 1992, p. 91.

102 Bastide et al. 1989; Brun 1992; Rohrmann 1999; Sjoberg 1996; Slovic et al. 1980.

103 Epstein 1994; Slovic et al. 2002; in press 2003; Sloman 1996.

104 Bargh 1984; Clore and Gasper 2000; Damasio 1994; Frijda et al. 2000; Zajonc 1980.

105 Finucane et al. 2000; Jackson et al. 2004; Loewenstein et al. 2001.

106 Murdock et al. 2003.

accounts of events influence lay interpretations of risk.[107] 'Risk signatures' can become grounded in everyday experience and the more they are grounded, the more they are seen as personal and credible threats.[108]

Empirical accounts of the narrative structure of risk communication demonstrate that whereas experts see risks as chains of cause and event, lay people tend to see them in a social context of relationships.[109] Research is needed to assess the importance of these insights in the context of cyberspace.

1.7 Trusting in Cyberspace

Trust is a means for alleviating risks, but there is only a weak empirical foundation for assessing the basis upon which people are prepared to trust others in cyberspace or to trust in the trustworthiness of ICT systems. It is clear, however, that growing numbers of interactions are occurring between strangers who have never met 'in real life' and exchanges of a social and commercial nature are clearly increasing, indicating that whatever the explanation of the basis for trust, people do act as if they trust 'virtual' others in many instances.

For example, in the commercial world, people are buying and selling goods from each other on eBay, spending hours playing computer games, and dating via instant messaging. Massively Multiplayer Online Games (MMOGs) involve increasing numbers of people in buying and selling imaginary 'property' and avatars. Game players have invented a currency for exchange, the total value of which in 2001 was estimated as equivalent to the GDP of a relatively wealthy country.[110] More and more government services are being provided online, giving rise to new means of accessing information and of communicating between all the actors in the social system.

Box 14 Trusting in Cyberspace

Trusted connections between machines: is your computer connecting to the one you have asked it to? Is the connection secure? Is your security being compromised by the other system?

Trusted, verifiable content: are you sure that the content you are downloading is real rather than pirated? If you are downloading from a specific site, can you verify that the site is the one you think it is?

Trusted transactions: are you confident that any transactions and credit card (or other private) details are secure? Or, at least, that you are aware of the level of security that exists? [111]

These relationships are possible only to the extent that people behave as if they trust in each other and in the systems they use. Issues of trust involve person-to-person, person-to-system, and system-to-system trust. The former two are emphasised in this section (the latter has been addressed already in section 3). Box 14 highlights questions that are often asked about trusting in cyberspace from the end-user's point of view.

Cyberspace Trust and Expectations

Trust is a critical factor for the acceptance of electronic services including those provided by electronic commerce and e-government service providers. Research in the fields of human-computer interaction (HCI) and computer mediated communication (CMC) focuses on increasing

107 Petts et al. 2001.

108 Horlick-Jones et al. 2003.

109 Wiedemann et al. 2003.

110 Tyrrell 2004.

111 Summary of Key Themes and Issues, Foresight Expert Workshops, November 2003.

people's trust perceptions, rather than on enabling people to make reasonable decisions about what or whom they may trust in cyberspace.[112]

The need for a trust framework for understanding online commercial interactions has been recognised in this literature to differentiate between situations requiring different types and levels of trust.[113] In the case of electronic commerce, the trustor may have to wait for days or weeks to take possession of goods and check that they are satisfactory. Interactions in cyberspace may be perceived as being riskier and have a greater need for trust than similar interactions in a physical context. Whether people are prepared to engage in a relationship has been found empirically to depend on many factors including the following:

- The number of actors involved in the exchange (ranging from a single pair to potentially millions in public good dilemmas).
- The actor type (individuals, organisations, technology).
- Whether there is synchronous or asynchronous trust exchange (strategic insecurity).
- Whether the user can identify trust-warranting properties.
- The types of signals employed to communicate trustworthiness (symbols and symptoms of trustworthiness, identity- and property-signals).
- The person potentially placing trust, including propensity to trust, knowledge of the situation, prior experience, potential benefits they expect, and the risk they face (enacted as 'trusting action').[114]

Trust needs to be a core concern in the design and deployment of cyberspace technologies and it is being acknowledged more widely today that technical systems can only work as part of a larger socio-technical system.[115] Trust appears to reduce the need for costly control structures, and makes social systems more adaptable.[116] Information exchanges that are now being mediated by technology or even executed with technology as a transaction partner, put more responsibility for supporting trust on the designers and operators of the technical systems.[117]

Game Theoretic and Institutional Approaches to Trust

From the vantage point of game theoretic models, trust can be conceived as arising out of expectations. This body of theory indirectly informs much of the thinking about the future role of software agent-based computing in cyberspace. We examine theoretical arguments about trust developed in the economics discipline next.

Trust is a matter of *expectation* –a trusting individual has some opinion about what might happen, some notion as to how likely the various possibilities are, and some belief about how these outcomes and their likelihood are affected by his or her choices. Various models of choice that take account of the probabilistic nature of risk may be used to represent these assessments. Trust may also involve more or less *consequentialism,* i.e. it may be bound up with the process as well as the outcomes. For example, an online customer may trust a transaction without distinguishing between the (distinguishable) reliability of the merchant, the payment and/or delivery services, and the legal mechanisms that provide compensation in the event of loss. Trust has been a difficult concept for

112 Sasse 2004.

113 Corritore et al. 2003; Egger 2001; McKnight and Chervany 2000; Riegelsberger and Sasse 2001; Sasse 2004.

114 Riegelsberger, et al. 2003; Sasse 2004.

115 Checkland 1999.

116 Uslaner 2002.

117 Reigelsberger et al. 2003.

economists to clarify,[118] but its influence is widely acknowledged.[119] Considerable research focuses on the development of game theoretic approaches (see Box 15).

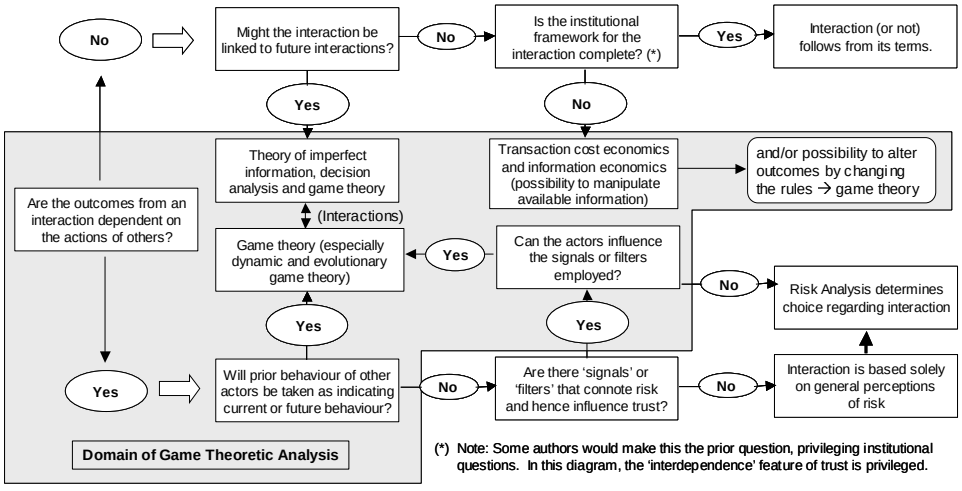
Box 15 Games and Incomplete Information

Decisions to interact with other individuals for gain or loss, e.g. buying and selling, employments, co-operation for purposes of mutual gain, etc., are conceived by economists to be 'games'. A decision to 'play' in a game, if alternatives are available, in essence, involves trust: one trusts that the interaction is as described, that the other player(s) (actor(s)) will behave as expected. This trust is essentially an expectation – an assessment of what will happen in the future and in different contingencies. When individuals regard other actors as unresponsive or unpredictably responsive to their choices, the economic analysis of incomplete information is used to analyse the interaction. When individuals see their choices as being interdependent, the appropriate economic approach is *game theoretic*.[120]

A basic framework for distinguishing game theoretic from information and institutional economics frameworks is illustrated in Figure 2. Game theoretic analysis applies when the institutional framework, including laws, rules, norms, and standards, is incomplete because strategic actions will affect the institutional framework. Such analysis is not relevant where interactions cannot be affected by others' actions.

An alternative approach that de-emphasises the role of game theoretic analysis focuses on the institutional structures – laws, rules, norms, and standards - that are imposed on market players and govern their interactions.[121] The fields of transaction cost economics and 'new' institutional economics both acknowledge that long-term contracts are often incomplete. When parties are mutually dependent on the maintenance of business ties there is a strong incentive not to defect or behave opportunistically. This incentive amounts to what some would call 'trust'.

Figure 2 The Domain of Game Theoretic Analysis



Source: Steinmueller 2003.

118 Hollis 1998.

119 Cave 2004.

120 Cave 2004.

121 Williamson 1975.

122 Cave 2004; Steinmueller 2004; Williamson 2000.

Economists focus on the costs of breaching trust as the principal motive for maintaining it.[123] Trust serves as a 'lubricant' in markets, reducing transaction costs and assuring something closer to perfect competition. The institutional framework for cyberspace transactions involves the use of technical methods for user authentication, time-stamping and electronic signatures; and norms or standards, such as indemnification from fraud. These can reduce the costs of transactions and make them more likely to occur.

Economists also draw a distinction between *trusting* – whether I should trust another entity (person, group, institution, etc.) and *trustworthiness* – whether another entity should trust me. Despite the normative connotation of the words (relating to a standard or norm), these terms are used to reflect behaviour – one acts *as if* one is trusting or acts in a way that is consistent with eliciting trusting behaviour from others (trustworthiness). Choices that are made concerning whom to interact (play) with, and whose expectations to fulfil, disappoint or ignore, determine the 'network structure' of the game.[124] In game theoretic contexts, it is relevant to consider how the design of the game itself embodies trust especially where contracts may be incomplete.[125] Trust is essential to the functioning of norms and standards that allow markets to function.

Trust in games can be analysed with reference to all the underlying data of the game: the set of 'players'; their strategies or powers of action; their information; their motivations or pay-offs; and the solution concept used to summarise the information in the game. A common assumption is that the other players engaged in a game act rationally which allows their behaviour to be predicted. Much recent work represents trust as a strategic choice that is influenced by the credibility of information, i.e. its provenance, and the degree to which others will believe our own communications, e.g. threats and promises.[126] Research also suggests that the distribution of trust is a key factor in agent behaviour (see Box 16).

Box 16 The Distribution of Trust

Trust (trustworthiness and trusting behaviour) is a valuable property of complex interactive systems. From the economic point of view, it is not the level that matters so much as the *distribution* of trust. How trust is distributed governs expectations and the alignment of information, motivation and the power to act. A simple policy of maximising trust may be myopic or even counterproductive. For example, customer trust in electronic commerce systems is advantageous, but it does not follow that more trust is better – a higher level of trust increases the possibilities for opportunistic behaviour of those who are trusted.[127]

Simple games representing stylised views of trust and their associated equilibria can be used to model agent behaviour as strategic behaviour; as the formation of player networks; and as hybrid games that combine elements of both approaches.[128] A basic approach to game theoretic analysis is given by the *coordination game* in which players choose between high trust and low trust strategies. In such games, individuals are assumed to choose a single strategy for all their

123 Cave 2004; Steinmueller 2004; Williamson 2000.

124 Jackson and Watts 2002; Morris1997.

125 Bacharach et al. 2001; Bacharach and Gambetta 2001; Bowles and Gintis 2000.

126 Bowles and Gintis 2000; Guerra and Zizzo 2002; Hardin 1991.

127 Cave 2004.

128 Cave 2004.

interactions.[129] This framework may be extended to consider a multiple period game in which cooperation or defection is a choice in each period for each player.[130]

Games can be used to suggest outcomes in terms of whether high trust or low trust equilibria pertain if all players interact with each other in a fully connected network. Trust is partially a collective property, depending on how individuals are linked, whom they trust and who trusts them. It is feasible to look at the influence of linkages of trust to see whether networks will form that provide optimal trust. These approaches taken by economics to understanding trust or agent expectations are mirrored in the modelling of software agent-based behaviour in cyberspace and the way trustworthiness may be signalled (see Box 17 and section 5.1).

When trust and crime are important there are *externalities*. These can be mitigated by *precautions* taken by the affected parties. The collective response (in civil, criminal or contract law) to market failure is to align the nature and amount of precaution with the assignment of liability for consequences.[131]

Box 17 Signalling Trustworthiness

Economic theory relating to product safety and reliability distinguishes two strategies to signal trustworthiness. A firm wishing to convince customers of its reliability can provide extensive or minimal warranty protection. In the former case, the signal is credible because the warranty would be too expensive to offer otherwise (providing the assurance is reliable and inexpensive to exercise). The customer does not need to trust the firm, but the firm may need to trust the customer not to make frivolous claims. A well known firm can credibly signal trustworthiness by providing unusually low levels of protection, since it places its reputation on the line by so doing.[132] Trust in this interpretation is solely about the assessment of risk because the consumer has little control over the allocation of risk. Trustworthiness signalling can influence agent expectations.[133]

Varian considered the impact of liability on the incentives to offer a public good, such as ICT system reliability or trustworthiness.[134] The results depend on how the provision of the public good relates to individual effort. They also depend on whether decisions to contribute to the provision of this good are taken simultaneously or in sequence. This has implications for the risks associated with computer viruses, spam and harmful or illegal content in cyberspace.

Precautionary activities, themselves, have externalities. Some have the effect of protecting others, e.g. shutting down the offending communication. Some do not affect risk to others, e.g. protecting one's own machine. Others may transfer the risk or costs to others, e.g. attacking those who appear to have sent offending messages. These issues interact with issues of industrial structure because they influence and are influenced by the degree of monopolisation in the market. They also influence the prevalence, adequacy and ownership of standards and the nature of networking among market participants.

In summary, in the economic view of trust, trust serves as a useful lubricant for establishing and maintaining networks of agents involved in activities in which mutual gain is a possibility. Achieving

129 Axelrod 1984.

130 Cave 2004.

131 Shavell 1987.

132 Cooper and Ross 1985; Gal-Or 1989; Lutz 1989.

133 Cave 2004.

134 Varian 2002.

an overall increase in the level of trust is less relevant in achieving efficient outcomes or stable networks than is the *distribution of trust* that supports the setting of priorities for establishing trust relationships and that establishes a structure for negotiating the liabilities arising from interactions. Networks involving trust will tend towards equilibrium involving a high level or a low level of trust and agents will either rely on consistent behaviours or expect opportunistic behaviour. Aligning the institutional rules of cyberspace networks with the tendencies of a network may improve efficiency. The possibility of free riding may reduce the quality of the public good such as system dependability. Because it is possible for the independent actions of one member of a network to compromise the interests of others, cyberspace networks may need stronger rules for exclusion or for taking sanctions against participants that breach the trust of others.

1.8 Trust and Social Capital

Trust is a major component of 'social capital'.[135] Bourdieu and Passeron developed the idea of 'social capital' as a means of modernising Marxist concepts of 'class' reflecting the relational capital of elites.[136] This concept can be linked to the positive effects expected from networks of trusted agents. The social capital idea has received considerable attention due to the efforts of Putnam.[137] He sought to explain differences in economic performance between Northern Italy and the mezzogiorna region and between regions within the US as the result of differences in the nature and density of non-economic relational associations in society.

Although many economists are sceptical of the social capital idea because of the causal ambiguity in the relation between non-economic social relations and economic performance,[138] some economists have embraced the idea to explore 'trust' as a feature of preferences.[139] It can be argued that societies that engender and support a more complex and dense pattern of networked social relations may benefit from lower transaction costs and more robust assumptions about the unlikelihood of opportunistic behaviour. This approach helps to understand how 'trust' can be extended between parties that are capable of opportunistic behaviour by creating a 'web' or 'network of trust'.[140] This would suggest that policies aimed at supporting the development of virtual communities in cyberspace would have a positive payoff in economic performance.[141]

This view is not uncontested since some would argue that the concepts of contract and trust are antithetical. Others point to a pragmatic inconsistency. Trust in incomplete contracts involves acting on the basis of incomplete information. Many trust-enhancing measures, e.g. authentication mechanisms, add information and actually *weaken* trust. Contracts exist in a specific legal and social context that provides for monitoring, verification and enforcement. Where enforcement involves relationships between actors, hierarchies or other complex structures of trust may emerge which introduces further complexity into the analysis of trust and economic performance.[142]

One reason that there are such differing perspectives on trust in cyberspace is related to whether the analysis of behaviour begins from an individualistic or egoistic perspective or from a collective or societal perspective. This raises ethical issues, some of which we outline in the next section.

---

135 Fukuyama 1995; Politt 2001; Putnam 2000.

136 Bourdieu and Passeron 1977.

137 Putnam 1993, 2000.

138 Sobel 2002.

139 Glaeser et al. 2000; Knack and Keefer 1997.

140 Mansell et al. 2000.

141 Mansell and Steinmueller 2000; Steinmueller 2004.

142 Eisenstadt and Roniger 1984.

1.9 Ethics and Cyberspace

Technologists sometimes make a distinction between the 'real' world and cyberspace. The spaces, feel, channels and access may be quite different, but research increasingly shows that many aspects of human behaviour remain constant.[143] It seems unlikely that the majority of people will alter their basic behaviours, ethical stances and morality when they enter cyberspace. In fact although criminals – or those who seek to exploit others – will think of new forms of attack, most people are likely find ways of translating conventionally understood norms and practices into cyberspace. When people understand that there are certain ethical and moral requirements, they may be more likely to adopt and demand them. Helping them to acquire that understanding is a key challenge for crime prevention.

For this reason, we need to consider the ethical standpoint from which it is feasible to argue that interventions in cyberspace to improve crime prevention are reasonable. O'Neill argues that a critical approach to practical reason 'does not take the expression of the basic norms of a community or of one's own personal commitments as intrinsically rational'.[144] Instead, the standards for taking action should be whether the guidance provided to those with a capacity to act can be recommended universally without damage to others and whether they can be understood. Any measures to secure cyberspace through building trust and trustworthy systems raise numerous ethical issues. Standard ethical concepts map onto cyberspace in interesting ways.[145] This section reviews ethical positions with respect to attempts to secure cyberspace.

Trust and Security

In earlier sections we have seen that there are many definitions of trust and many perceptions as to likely actions under conditions of uncertainty in cyberspace. An enticing means of reducing uncertainty in cyberspace is to develop and implement security systems but this raises ethical issues around the spread of a security infrastructure. What avenues will be cut off for those who do not wish to employ it? In section 3.3 we discussed the way security systems require some kind of identity authentication. However, for many users, the charm of the Internet is precisely the ability to get away from, or play with, one's identity. Every extension of power should require a justification and agreement as a result of a dialogue,[146] and the software code of the Internet controls its architecture and what actions are permissible.[147]

To question the extension of cyberspace security there needs to be a forum where the sceptical can table their requirement for justification. However, given the global reach of the Internet enabling security measures to jurisdictions, then enabling a full cross-section of users to debate is very difficult. One strategy may be to place the burden of proof on those who wish to alter the principles upon which the Internet was founded, i.e. namely liberty and openness. On the other hand, from an argument based on John Stuart Mill's work, *On Liberty*,[148] it could be held that liberty and openness are the essentially important values *after* a certain level of cultural development has been achieved. This might imply that it is first of all essential to provide a cyberspace architecture in which privileged activities – selected on the basis of judgement by those with political power - such as science and commerce, can flourish, and only then should liberty become an overriding value.

---

143 Hawkins et al. 1999, Mansell and Steinmueller 2000; Silverstone 2003.

144 O'Neill 2000, p. 26.

145 O'Hara 2004a.

146 Ackerman 1980.

147 Lessig 1999.

148 Mill 1869.

Rationality and Value

In the context of cyberspace, one notion of trust is a utilitarian notion developed by Luhmann.[149] This sees trust as a way of reducing complexity, by accepting the bona fides of agents rather than investigating them. The second is a moral notion of trust developed by Durkheim, which sees trust as an inclusion into a value-laden society;[150] if I trust you, I accept you as one who shares my values.[151] Durkheim's view is optimistic and conservative; Luhmann's is rooted in self-interest. The Luhmann view is that trust is the effect of good behaviour, and therefore ensuring trust requires providing incentives for good behaviour. The Durkheim view is that trust is the *cause* of good behaviour, and that the best strategy to ensure that people behave well is to trust them, and make it clear to them what behaviour is acceptable.

This argument mirrors a major ethical debate about the purpose of the Internet and the limits of its regulation. Castells and others argue that openness is deeply embedded in the architecture of the Internet.[152] They suggest that cyberspace technology is inherently supportive of values such as passion, freedom, social worth, caring and creativity; values that are prevalent within the 'hacker' community. They argue that these values need to be defended in the face of efforts to achieve control for purposes such as crime prevention.

Others suggest that the picture is more complicated.[153] While evidence shows that civil society organisations are making much greater use of cyberspace tools, the extent to which such use is dependent upon maintaining all of the original features of the Internet's architecture is unclear. In addition, many uses of the Internet may be associated with actions across the spectrum of values and political aims. The relationships between the spread of the Internet and issues of privacy, vulnerability and security in the broader context of ethical and political considerations, mainly in the United State s, have been considered.[154] In the UK, and with a more international orientation, some empirical work has been undertaken on the use of the Internet for criminal activities, but it tends to focus on near-term developments and technologies rather than on the technological landscape that is likely to emerge in the coming decades.[155]

Some argue that the governing values of the Internet, liberty and openness, are a stage through which the Internet had to move, but which may be transcended to allow other cyberspace activities such as commerce. Others argue that liberty and openness are essential and non-negotiable. The former group wants to ensure trust by altering cyberspace architectures to make bad behaviour more difficult. The latter want to be allowed to imbue the Internet with their libertarian values. These two groups disagree about what constitutes good cyberspace behaviour and good faith and about when it is in one's interests to trust.[156]

149 Luhmann 1979; and O'Hara 2004b.

150 Durkheim 1893.

151 O'Hara 2004b.

152 Castells 2001; Himanen 2001; Lessig 1999; Miller 2003; Naughton 1999.

153 O'Siochru 2003; Surman and Reilly 2003.

154 Latham 2003.

155 Thomas and Loader 2000; Wall 2001.

156 O'Hara 2004a.

Trust and Rationality

There is also a spread of views about trust and rationality. The reciprocity required by trust is part of the uncertainty that trust tries to dispel. Under what conditions is it rational to assume that reciprocity will be respected? The narrower the conception of when it is rational to trust, the lower the level of trust in a society, and also the lower the level of betrayal.

Position	Representative	Implications
Law of the jungle		Trust depends on the principal's assessment of the agent. As there is little or no comeback for the principal if the relationship goes wrong, then trust may be slow to develop. However, it does depend on the type of relationship. Relationships that thrive on openness and selflessness (such as friendship, e.g. in a chatroom or a MUD or MOO) will do well; those were the protagonists have more distance, such as commercial relationships, will not thrive.
Leviathan	Thomas Hobbes (1588-1679)	A strong state – Leviathan - will provide an important resource for bootstrapping trust. A central authority with stern powers of sanction will tilt the balance of probabilities towards trustworthy behaviour, and away from betrayal. People may still betray if they think they can get away with it.
Preference models	David Hume (1711-1776)	The important psychological vectors are preferences and calculation. We form preferences, and then we calculate how best to achieve them. If we can theorise about and calculate others' preferences this will help trust and work out when security solutions are to the advantage of all.
Out of equilibrium play	Adam Smith (1723-1790)	The game theoretic notion of 'out of equilibrium play' or making the strategic choice that is not the best answer to your opponent's move. The actors need to have alternative motives to simple preferences; they need to be motivated by views about outcomes that are best for others, and impartial between themselves and others.
Fairness	Immanuel Kant (1724-1804)	Insist on fairness across agents. One should not treat another any differently from the way one would have oneself treated.
The General Will	Jean-Jacques Rousseau (1712-1778)	People generally will judge their interests in terms of the interests of their society (i.e. an online community). Free riding will be a relatively small problem; most people most of the time will allow the interests of the community to trump their personal egoistic interests.

Table 4 Positions on Trust and Rationality

Source: Adapted from O'Hara 2004a.

Table 4 suggests that as we move down the table, positions on this issue become more forward-thinking and less egotistic.[158] There are many difficulties in these positions and many have been sceptical that they could sustain or nurture trust.

These positions are all defined in terms of how egotistical the actors are assumed to be and how their identities influence their motives. Where identity is highly fluid as in cyberspace and subject to different conceptions, there is scope for very different views on cyberspace and its governing values.[159]

Liberalism and Liberty

Another ethical issue concerns the question of how much western bias informs debates on and policies for crime prevention and the security of networks. The idea that environments are definable in terms of local features (all of which may be virtual) stems from the philosophy of

157 Hollis 1998, O'Hara 2004b.

158 Hollis 1998, O'Hara 2004b.

159 O'Hara 2004a.

Descartes. The idea of people as individuals – and therefore of identity as something that can be fluid, and self-defined – is notably western. Many argue that such positions cannot be sustained without threat of severe social breakdown and that the social context of interactions must be taken into account.[160] The positions outlined in Table 4 are all characteristically western liberal positions. Those that argue against western liberal hegemony assert that treating people as egotistical or of equal value is unrealistic. There must be some intermediate position.

One line of argument is a principled one, which states that the essential aim of authorities should be to allow any actor to pursue his or her own conception of the good (if this does not interfere with others).[161] For cyberspace this means architectures allowing maximum freedom, including the freedom to be illiberal.[162] This position takes liberalism as a universal ideology although it is a western-centric idea. The second line of argument is pragmatic and conservative; liberal culture dominates the Internet and departing from liberal western principles would be a nod too far towards a multicultural agenda. Hence, western concerns about organised crime, cyber-terrorism, or the growth of electronic commerce, should come first, even if other users are to be respected. The third response is a compromise. Liberalism's conception of the 'good' is rooted in rights but all parties around the world may not agree these. Retreating from the rights-based discourse, the issue becomes what privileges people should have in cyberspace. This, in turn, becomes a political problem in response to which a compromise may be reached.

It is essential to allow access for non-western representatives to such negotiations on how to promote cyber trust and enable crime prevention. Positions on this ethical issue are closely linked to the role of the media and strategies for building awareness of the risks in cyberspace and about trust in cyberspace. If there is a need for an informed and reasoned debate in society, citizens need to be better informed about crime associated with cyberspace and about the way the Internet is permeating our lives. But there is a risk that concerns about cyberspace will become amplified. Thus, two uncertainties lie at the heart of the ethical dilemma – how will the general population engage in such a debate and how will the media report the issues?[163]

1.10 Implications for Cyberspace Trustworthiness and Trusting Behaviour

Models for understanding trust between individuals or human agents of individuals operate within well-established social and ethical contexts. In the preceding sections we have seen that different assumptions underpin models developed within different disciplines. The advent of cyberspace raises the question as to whether any distinction should be made between *online* and *offline* trust. Human societies support numerous contexts for trustworthiness and trusting behaviour and cyberspace adds new dimensions in that it may involve varying combinations of agents (we examine two cases where this applies in section 5).

- Two human agents
- A human and an artificial agent
- Two artificial agents
- One or more artificial proxies for human agents

The metaphor of trust in cyberspace could become over extended, but without such a metaphor, linkages with social and economic behaviour would be difficult. Cross-disciplinary research

160 Gray 1995; Mahbubani 2002.

161 Ackerman 1980; Rawls 1972.

162 Manasian 2003.

163 This issue is discussed further in section 7.5.

between the software engineering disciplines and the social sciences is needed to understand these linkages.[164]

As indicated in section 4.4 it is uncertain whether a utilitarian or a moral notion of cyberspace trust is appropriate and whether they are mutually exclusive within the context of using cyberspace environments. We may take a utilitarian view when carrying out financial transactions, but a moral one when considering sharing open source software. This issue may affect approaches to digital rights management software. One view would be to treat it purely in utilitarian transactional terms, whereas the other would be make the content available for the common good but to monitor and punish any abuse of agreed ethical principles.

The nature of trustworthy *knowledge acquisition* in cyberspace is poorly understood (see section 5.2). A number of approaches exist in the offline world but it is not readily obvious that they translate to the cyberspace environment. The scale and volumes of information to be acquired in the future are such that within the technologies being developed some understanding of the trustworthiness of the acquisition processes needs to be developed to contribute to trusting behaviour.[165]

In summary: 1. perceptions about the dangers of cyberspace are influenced by the media and people's social networks which may amplify or attenuate such perceptions; 2. trust in cyberspace depends upon many factors that need to be understood by technology developers and other stakeholder; 3. economic models of trust provide insight into the behaviour of human and non-human agents in cyberspace; aligning the rules of networks with the distribution of trust may improve the efficiency of cyberspace interactions; 4. the development of social capital is an important consideration in fostering trusting behaviour; and 5. there are very different views about whether actors in cyberspace will follow their self-interest or other motivations.

164 O'Hara and Shadbolt 2003.

165 O'Hara and Shadbolt 2003.

5 APPLYING TRUST MODELS IN CYBERSPACE

Two technology developments that are likely to be critical for the future development of cyberspace are the deployment of software agents and the development of the semantic web. In this section, we examine each of these to see how concepts of trust and risk are being modelled and whether there is reason to be concerned about knowledge management processes in cyberspace.

In the preceding sections, it is clear that if future ICT systems are to become more dependable and secure there will need to be changes in the design and implementation of ICT components, hardware and software. They will need to become more reliable and trustworthy themselves. Many modern computer applications are open distributed systems in which the (very many) constituent components are spread throughout a network in a decentralised control regime that is subject to constant change throughout the system's lifetime. Examples include peer-to-peer computing, the semantic web, the grid, web services, e-business, m-commerce, autonomic computing, and pervasive computing environments. In all of these cases there is a need to have autonomous components that act and interact in flexible ways in order to achieve their design objectives in uncertain and dynamic environments. Given this, agent-based computing has been advocated as the natural computation model for such systems (section 5.1).[166]

Knowledge technologies and the semantic web are enabled by recent technological developments that allow much more intelligent machine engagement with the documents, services and other objects on the World Wide Web. They manipulate and create knowledge, i.e. usable information in a context, and we take developments in this area as a further case study to illustrate how concepts of trust are being applied that influence the future of cyberspace (section 5.2).[167]

1.11 Agent-based Systems and Trust

The application of autonomous software agents, sometimes representing their human owners, in large-scale open distributed systems presents a number of new challenges. We focus specifically on the challenges that relate to the interactions in such systems. How do agent-based system designers decide *how* to engineer protocols (or mechanisms) for multi-agent encounters? How do agents decide *whom* to interact with? How do agents decide *when* to interact with each other?

As the discussion about trust in section 4 has shown, it is impossible to reach a state of perfect information about the environment and the interaction partners' properties, possible strategies, and interests. Agents are faced with significant degrees of uncertainty in making decisions. Agents have to *trust* each other in order to minimise the uncertainty associated with their interactions, e.g. a buyer has to trust that a seller will deliver goods in time, or a seller will have to trust an auction house to sell its goods at the highest possible price).[168] Trust can be defined in this context as:

> 'A belief an agent has that the other party will *do what it says it will* (being honest and reliable) or *reciprocate* (being reciprocal for the common good), given an *opportunity to defect* to get higher payoffs'.[169]

In designing agents and open multi-agent systems, it is important to distinguish between *individual-level trust* (an agent believes its interaction partners are honest or willing to be reciprocal) and

166 Ramchurn and Jennings 2004.

167 O'Hara and Shadbolt 2004.

168 Ramchurn and Jennings 2004.

169 Ramchurn and Jennings 2004.

system-level trust (actors in the system are forced to be trustworthy by the rules of encounter, i.e. protocols and mechanisms, that regulate the system).

Individual-level trust between agents requires endowing them with the ability to reason about the likely reciprocal nature, reliability or honesty of their counterparts. *Trust models* aim to enable agents to calculate the amount of trust they can place in their interaction partners. To calculate the degree of trust, agents need to gather some knowledge about their counterparts' characteristics in many different ways, e.g. through inferences drawn from the history of outcomes of multiple direct interactions with these partners or through indirect information provided by other agents.[170]

System-level trust concerns the design of protocols and mechanisms of interactions, i.e. the rules of encounter, including security. These interaction mechanisms need to be devised to ensure that those involved can be sure they will gain some utility if they rightly deserve it, i.e. a malicious agent cannot tamper with the correct payoff allocation of the mechanism. We expect agents to interact using a particular mechanism only if it can be trusted. This highlights the need for protocols that ensure that the participants will find no better option than telling the truth and interacting honestly with each other.[171] The state-of-the-art in this area with respect to multi-agent software systems is shown in Box 18.

Box 18 Trust in Multi-agent Software Systems

Trust models based on sociology, machine-learning techniques, and game theoretic approaches have been shown to be useful in helping software agents to interact better. As indicated in section 4, these models each look at different facets of the trust problem without relating to each other. A very small number of interaction protocols have been shown to be trustworthy because the computational complexity of interaction protocols can be a barrier to designing trustworthy interaction mechanisms.

Security mechanisms provide a number of techniques to make secure interactions. However, they do not control the semantics of interactions beyond the line of defence provided by security policies and encryption techniques (see section 3). Most trust models and interaction protocols do not cope effectively against strategic lying by agents. Most trust models and interaction protocols are not collusion-proof and agents can collude in order to exploit other agents or the system itself.

Game theoretic approaches to studying interactions, require protocol designers to make many unrealistic assumptions about the environment and the social network. A more precise modelling of the context of interactions is needed and trust models and interaction protocols should be adapted to the dynamic context in which they are used.[172]

With the advent of open distributed systems, agents representing different countries, institutions, or societies, will be interacting. This could give rise to a clash of norms and cultures, e.g. laws, societal norms, that will result in software agents making the wrong assumptions about their counterparts, leading to distrust. Agent-based trust models in the future will need to conceptualise differences in expectations arising from differences in norms and cultures. One aspect of this challenge concerns the relationships between the data that agents encounter or collect and their meaning. We examine developments in knowledge technologies next.

1.12 Knowledge Technologies and the Semantic Web

The major concerns for trust in cyberspace environments resulting from developments in this area are: 1) making sure that the input to knowledge and information manipulation processes is

170 See Figure 2 on game-theoretic approaches to trust and von Neuman and Morgenstern 1944.

171 Ramchurn and Jennings 2004.

172 Ramchurn and Jennings 2004.

trustworthy, and 2) ensuring that the processes themselves are trustworthy, and their limits and margins for error are known and predictable.[173]

Operationalising the concept of trust can be accomplished in many ways in the context of knowledge technology development. The goal is to create or maintain trust in the cyberspace domain. Some approaches can be characterised under the heading *tactics for trust* (see Table 5).

Table 5: Tactics for Creating or Sustaining Trust

Tactic	Description	Costs
Transparency	Allow principal access to hitherto closed processes, black boxes.	Potentially open to creating mistrust, if expectations are too high.
Transfers of ownership	Allow stakeholders decision rights and responsibilities.	Stakeholders may be more reluctant to put in effort than an agent.
Exploiting transitivity of trust	Where a trust network already exists, extend it via transitive (or, on occasion, distributive) extensions.	Neither transitivity nor distributivity is a perfect model of trust. Plus this strategy cannot address any bootstrapping problem.
Certification	Create some institutional support for digital signatures, thereby securing provenance.	Institutional structures are contrary to the anarchistic value ethos of the net, and thereby might work to reduce trust (cf Durkheim). Does not address bootstrapping, as the principal still has to trust the certification system and authorities.
Restriction	Increase trust by policies designed to avoid interaction with the non-trusting.	May be arbitrary. May be over-limiting. Hard to evaluate the efficacy of the tactic.
Formal methods	Use formal methods to avoid dealing with the scruffier parts of the web.	High modelling overhead. Plus the whole development of the web, with its heterogeneous users, has encouraged scruffiness. Many of the richer parts of the web are scruffy.
Calculi of trust	Use formal characterisations of trust relationships to govern when an agent should trust.	Trust, being a second-order phenomenon, is hard to model successfully. Such a system is likely to lack the flexibility inherent in trust.
Interrogation	Submit documents, web pages, etc, to interrogation and scrutiny.	Technology in the early stages.
Knowledge management	Use tools for knowledge management to maintain knowledge bases and keep them accurate, up to date and trustworthy.	High maintenance overheads.

Source: O'Hara and Shadbolt 2003.

As Table 5 shows there are costs and benefits associated with each of these tactics for establishing or maintaining trust. Using knowledge technologies to *manage knowledge more effectively* implies the need for *improved* knowledge technologies. This, in turn, requires a better understanding of the knowledge technologies that will be implemented in the future and in part focusing research on them on this area of application. At present the technologies are immature so

173 O'Hara and Shadbolt 2004.

the cost of ownership is high. As they become better automated and 'trustworthy', it is expected that this cost will decline and their use will expand.

The tactics for trust need to be combined in active *trust management strategies.*[174] As a counterpart to the human behavioural approaches to risk and trust management (see section 3.3.3), there is a need to maintain agile policies for managing trust where software is concerned. These include the collection of rich sets of *metadata* about knowledge sources and agents, and *ontologies* for expressing trust requirements. A physical analogy might be a library of books, catalogued by subject, authors and CVs, reviews of the books with reviewers credentials, cross references to other books not in the library with similar metadata for them, all linked and available at any time from any place. Such information needs to be dynamically and automatically updated as new sources are 'published'.

Maintaining the distinction between *trust* and *trustworthiness*, so that signalling trustworthiness does not become detached from trustworthiness itself is crucial. Corritore et al. argue that trust is an act by the principal and trustworthiness a property of the agent.[175] Where the principal and agent are 'software agents', such strategies are complex and demanding to maintain. We are already using primitive forms of such constructs in spam filters and privacy engines within browsers. It is also important to ensure that *functionality* is not sacrificed to trustworthiness. The scale of information resource that will be available online for social, economic and academic purposes is growing exponentially. Any strategy for trustworthiness has to take into account such growth. Ensuring that *privacy* is sufficiently protected so as not to undermine trust is clearly important as well (see section 6.2.1).

In the offline world *branding* and *reputation* work very effectively and it appears that they transfer well as contributors to trustworthiness in cyberspace. What is less clear is how fragile they might be and open to different forms of criminal attack that are not available in the offline world, e.g. mass attack, Denial of Service or masquerade. Effective procedures for the maintenance of knowledge bases will need to be developed to ensure that as sharing of knowledge in a controlled way becomes a major influence on commercial and social behaviour, the sources that are used are maintained and exploited in ways that ensure they can be trusted. At present there is very little understanding of the end-user's perspective on these issues. We examine the results of the first large scale survey in the UK which examined how the experience of users with cyberspace tools and applications may be influencing their ideas about trust and the trustworthiness of cyberspace.

1.13 Evidence of Trust in Cyberspace

A problem confronted by research aimed at examining end-user perceptions of trust and the trustworthiness of cyberspace is that, as in the case of operationalising trust for the development of software-agent based systems and knowledge management, it is difficult to define trust in a way that is meaningful for lay respondents to a survey.

Definitions based on rational expectations and game theoretic models are difficult to apply in social surveys. However, a conventional definition of trust can be used where is trust is defined as:

> '… a firm belief in the reliability or truth or strength etc. of a person or thing. ... a *confident expectation*. … reliance on the truth of a statement etc., without examination' (Oxford English Dictionary).[176]

174 O'Hara and Shadbolt 2004.

175 Corritore et al. 2003.

176 Dutton and Shepherd 2004.

This definition of trust allows for the possibility that the use of cyberspace technologies might undermine trust and prevent people from obtaining electronic services.[177] One possibility is that the use of the Internet will undermine trust because it eliminates face-to-face interaction. Empirical evidence on this possibility is sparse and contradictory. Some researchers argue that trust may be undermined in electronic interactions because the reduced communication channel makes it harder to observe non-verbal physical cues.[178]

There is no definitive research on the impact of different media on trust.[179] Trust might, in fact, be enhanced by making effective use of the vast amount of information and new forms of online social networks that are available through cyberspace interactions.[180] Generally, personalised interactions are perceived as being more trustworthy in the offline world than in cyberspace. Technology to support such interactions in a geographically independent way will become available in the near future. Understanding how this might affect trusting behaviour is likely to influence how these technologies are developed and operated.[181]

As suggested in Box 19, the relationship between information, uncertainty and trust is likely to vary along many dimensions including the extent of experience in using online forms of communication. If trust as conventionally defined is closely related to a greater level of certainty or confidence in the reliability and security of the Internet, it is likely that trust will be enhanced as a person learns more about the technology. However, it is also the case that information can create, rather than reduce, uncertainty.

Proximity or 'experience' with the Internet is one of many factors that could play an important role in perceptions of appropriate levels of trust in cyberspace. How much (dis)trust does the public place in cyberspace? How does cyber trust shape use of the Internet? In the US an empirical basis for examining the use and implications of the Internet for trust is being developed.[182]

Box 19 Trust in the Internet: The Certainty Trough

MacKenzie, a sociologist, suggests that there is a curvilinear relationship between information and certainty – a 'certainty trough'. Adapting his argument, it may be that those most socially distant from the Internet, with no knowledge of the technology or its use, are likely to be alienated from the technology and least certain about its role. Those who learn more about the Internet might obtain a higher level of certainty and trust in the technology. Those who are socially closest to the Internet such as ICT professionals may learn to experience higher level of uncertainty as they understand the issues around online reliability, security and privacy.[183]

The Oxford Internet Institute has conducted the first large-scale survey of Internet use in the UK, focusing on many issues including trust in cyberspace.[184] The results of the survey with respect to issues of cyber trust are summarised in Box 20.

177 Guerra et al. 2003.

178 Wallace 2001.

179 Johansen 1988; Rice 1984; Short et al. 1976.

180 Ben-Ner and Putterman 2002.

181 O'Hara and Shadbolt 2004.

182 Lohse et al. 2000; Lunn and Suman 2002.

183 Dutton and Shepherd 2004; MacKenzie 1999.

184 See http://www.oii.ox.ac.uk/research/?rq=oxis for the full survey results.

Box 20 First Oxford Internet Survey (OxIS) Results

Results based on a survey of 2,030 respondents participating in a multi-stage random sample of the population aged 14 and upwards in England, Wales and Scotland shed initial light on public perceptions of the trustworthiness of the Internet and how levels of trust are related to an individual's patterns of (non)use of the Internet over time.

Using the conventional view of trust as a 'confident expectation', the survey examined expectations about the reliability and value of the Internet and related ICTs. The survey revealed wide variations in cyber trust between individuals. Few exhibit a blind faith in the Internet, but most people are reasonably confident – if guarded – in the information and people they are able to access over the Internet.

Well over half (59%) of the respondents were using the Internet. This suggests that there is sufficient trust to support the continued diffusion of this technology, despite a general awareness of the potential risks entailed in exposure to unwanted mail, viruses and other potential risks.

The Internet does appear to be an 'experience' technology. Experience on the Internet tends to engender a higher level of cyber trust. Users of the Internet have more certainty and more confidence in the information and people they can access than do non-users, and many non-users have no opinion about the Internet's trustworthiness. Greater proximity to the Internet tends to instil more trust, to some extent (where 'proximity' is indicated by the use of the Internet over more years, in more ways and with greater expertise).

Those who are most proximate often become more sceptical and aware of potential risks, conforming to the 'certainty trough' model. The presence of cyber trust is positively associated with the use of the web for electronic commerce. However, those who use the Internet more, for example, for online shopping, are somewhat more likely to expose themselves to 'spam', e-mail and other bad experiences. This tends to undermine trust in the Internet and raise concerns about risks.

Individuals with more formal education tend to be somewhat more sceptical of the information and people accessible on the Internet, but also somewhat less concerned about the risks of Internet use.[185]

This research highlights issues concerning cyber trust for which more evidence and analysis is needed to gain a better understanding of the underlying social dynamics and learning processes. A surprisingly small percentage of users reported bad experiences on the Internet. This suggests that it is the right time, before problems with Internet use such as spam become more widespread, to take initiatives to reduce the likelihood of more users experiencing greater difficulties. Research on the co-evolutionary nature of human, organisational and technological systems is needed to underpin effective policies towards cyber trust and crime prevention.

All technologies are social in the sense that they are designed, produced, used and governed by people.[186] Understanding relevant social and institutional dimensions should be a key priority in addressing the way these technologies affect trust, crime and related issues.[187]

This is especially important because there is lower trust of the Internet among categories of users such as the less affluent who have less access to the Internet. For these groups, experience in using the Internet has a particularly disproportionate positive impact, increasing their trust in the Internet and lessening their preconceived concerns about risks. Education and exposure to the Internet may offer a general strategy for coping with the risks and threats to the perceived trustworthiness of this technology. However, education and exposure to ICTs are skewed towards

185 Dutton and Shepherd 2004.

186 Dutton 1999, Dutton et al. 2003.

187 Dutton and Shepherd 2004.

higher socio-economic groups. As a result, these strategies could reinforce the 'digital divide' in access to the Internet. Advances such as broadband Internet may exacerbate this divide. Initiatives to enhance the perceived trustworthiness of the Internet may be warranted, but such efforts will create a tension, competing against other values, such as privacy, which could be threatened by some trust-enhancing services (see section 4.4).

Other empirical evidence suggests that in many advanced industrial countries and in international organisations trust is a crucial factor that influences the future development of electronic transactions in cyberspace,[188] and that more needs to be known about the public's worries about how their personal information is used and protected.[189] Most survey research into attitudes towards privacy and the processing of personal data is of variable quality.[190] A MORI survey in 2003 in the UK revealed considerable public ignorance about what happens to their personal data when it is used by public agencies.[191] These studies need to be complemented by more comparable and systematic evidence about why people trust organisations, what specifically they trust organisations to do or not to do, how privacy attitudes relate to risk perception, and how people evaluate the trustworthiness of cyberspace and public and private organisations.

This section shows that: 1. software designers need to consider individual and system-level trust when they design multi-agent computer systems and that existing models of trust are inadequate; 2. no single tactic used in knowledge management technologies is sufficient to ensure appropriate levels of trust; and 3. there is a need for internationally comparative and systematic research on users' experience of trust and risk in cyberspace.

188 Raab 1998; PIU 2002.

189 6 1998.

190 Bennett and Raab 2003.

191 MORI 2003.

6 CYBERSPACE MARKETS AND POLICY CONTEXTS

Incentives for investing in the deployment of more trustworthy networks and ICT applications depend substantially on the dynamics of the market and the way it interacts with legislation (and its enforcement) and policy. We examine the economic drivers of cyberspace technology and service markets first and then the legislative environment in Europe, focussing particularly on privacy protection.

In order to understand the evolutionary dynamics that will influence how the technical components of cyberspace will develop in the market, we need to consider the special characteristics of these markets. Economic theory does this by focusing on expectations about the reputations and actions of firms who supply the technologies in the market (section 6.1).

The future of cyber trust and crime prevention in the UK also has to be considered in the light of the global context and, particularly, in the light of the impact of the existing legislative environment and crime prevention strategies. The need for additional measures, for new policy deliberation fora, and for investment in research must be addressed with full awareness of present constraints on and opportunities for crime (section 6.2). Deliberations about how to build trust in cyberspace, to alleviate perceptions of risk and to mitigate opportunities for crime invoke considerations of the need for, and feasibility of, both individual privacy protection and collective security. In section 6.2 we also focus specifically on privacy protection and the issue of social equity.

1.14 The Economics of Emerging Cyberspace Markets

An industrial structure, conduct and performance (SCP) analysis is helpful in understanding how markets are likely to evolve for ICT systems and services and the implications for cyber trust and crime prevention. The SCP framework is helpful in considering how reputation and the expectations that it engenders include market competition.[192] Because reputation and belief in this reputation, that is, trust, influence consumer decisions, firms have incentives to use trust as a way of creating or consolidating market power. From an economic viewpoint, reputation is constructed by prior experience while there always remains a possibility of exploiting reputation by engaging in opportunistic behaviour.

The asymmetry of information between firms and their customers can lead to customer 'lock-in,' reinforcing the emergence of dominant firms. Opportunities exist for influencing competition through the use or misuse of trust in horizontal, vertical and networked market relationships involving: 1) the construction or opportunistic use of trust, 2) the use of strategies to influence trust by attempting to 'signal' quality or risk, and 3) by changes to liability rules that assign risk and thus can either reinforce or obviate the need for trust.[193]

In *horizontal relations*, cyberspace changes the scope for collusive behaviour. Firms competing in electronic marketplaces have expanded opportunities for using anonymity to cloak departures from collusive agreements and, in some cases, a global platform for their activities. This could increase the likelihood of defection – and thus the need to rely on trust.[194] A second cyberspace influence is the scope for rapid and effective detection and response to defection due to improved information.

Trust may also be critical to *vertical* relationships, those involving input markets, access provision and retail sales to consumers, which involve search, payment, fulfilment and follow-up stages. New technologies have the potential to increase market competition by augmenting consumer search either directly, by empowering users, or, indirectly, through strengthening the capacities of

192 Cave 2004.

193 Cave 2004.

194 Belleflamme and Bloch 2001.

intermediaries. It is not obvious, however, that intermediaries will act solely in consumer's interests – they may seek to exploit consumers or collude with their suppliers. The way that the various components of market exchanges in cyberspace may favour concentration is suggested in Box 21.

Box 21 Forces for Cyberspace Market Concentration

Achieving trust in cyberspace *payments* favours the prominence of financial intermediaries. This may become a force for increasing market concentration. A firm's prominence also increases risk by making a larger target for fraudulent activities, i.e. 'phishing' attacks on online banking sites and transactions service providers such as Paypal.[195] Market prominence may reinforce concentration in the *fulfilment* phase where the selling party may be located in another (even an unknown) jurisdiction in which pursuing consumers' rights may be difficult or expensive. The *follow-up* stage of relations with consumers also highlights the importance of *signalling.* Verified information (e.g. quality certification by independent third parties) or assurance may advantage players with greater capacities to invest in these signals. This may favour increased market concentration.[196]

In competitive environments where the market is dominated by a small number of suppliers that are able to exert control over supply and price, i.e. oligopolistic competition, such as those characterising many cyberspace markets, firms may attempt to signal their *relative* trustworthiness by calling attention to problems encountered in doing business with their competitors. They may do so even though this may reduce trust in the market as a whole. Certification is an attractive alternative, but depends on the reliability of the certifying authority. Much recent literature on trusted third parties, cyber-notaries and Internet governance concerns the relative merits of competitive and coordinated certification.[197] While such third parties are regarded as essential to effective competition in electronic markets,[198] at present the effectiveness of a market in certification services is uncertain.

The increasingly heavy information content of goods and services delivered over the Internet is an important consideration for the evolution of cyberspace markets. They have the classic incomplete information problem.[199] A relatively high level of trust is required – perhaps on both sides – to fit such transactions into the relatively anonymous framework of retail commerce and this raises many issues for the technical means of securing identity and authenticity. In addition, cyberspace consists of many tiered networks and relationships and these have a major impact on the strength of demand for security precautions in the market. Demand for particular security solutions will be strongly influenced by the costs involved in switching between products on the market (see Box 22).

It is mainly market-led developments that will enable the spread and wider use of cyberspace technologies and influence their dependability. The rate at which technical developments leave the laboratory will be strongly influenced by the strategies of firms and the variety of products on the market. In turn, the legislative and policy frameworks that we examine next will influence the supply of and demand for more secure technologies.

195 Independent 2003.

196 Cave 2004.

197 Froomkin 1996, Gotoh 2003, Moreh 1997, OECD 2000, Smith and Keehan 1997.

198 Williamson 2000.

199 Incomplete information with respect to bargaining and contracts as compared to the assumption of perfect information and market equilibrium, see Cave 2004; d'Aspremont and Gerard-Varet 1979; Gibbons 1992.

Box 22 Networking and Switching Costs

A major source of *network relations* involves economic entities that produce complements rather than substitutes.[200] In a variety of cyberspace markets including software and telecommunication services, incumbents have an incentive to maximise, and potential entrants to minimise, the costs of '*switching'* between networks. 'Churn' can undermine trust in the stability of the market and reduce suppliers' incentives to invest in durability, dependability and continuity. Proprietary standards may serve to stabilise these markets at the cost of reduced market competition. The first-mover advantage of leading firms and the need to capture suppliers of complementary technologies or services may lead firms to reduce security barriers to developers, share information with them, and shift the cost, complexity and liability burdens of security to customers. Inferior security precautions may drive out good ones. [201]

Economic analysis tends to endogenise trust – to treat it as an aspect of the functioning of economic systems where the calculations are far removed from the intuitive notion of trusting behaviour. For individuals, the decision to trust another or to behave in a trustworthy way is analysed in terms of expected costs and benefits. The economic view of trust includes a rational commitment to limited rationality and to considerations of monitoring and enforcement. From this perspective, goods and services that enhance trust are valuable products and this extends to the provision of trust and identity services. These are information goods and the economics of incomplete information is relevant with its analysis of the problems of hidden information and hidden action. Institutions that permit credible or verifiable signals (assurance) and informal institutions (reputations) can improve efficiency, and specific contractual forms can align incentives. Trust is also a public good. A person cannot fully 'own' trust or exact payment for it and it is possible to 'free-ride' on the trust or trustworthiness of others. To the extent that trust is costly, it will thus be underprovided.[202]

Because trust is bound up with expectations, the incompleteness of information, of markets and of contracts, is critical. This suggests a role for self-regulatory mechanisms (e.g. open standards, reputations) and for appropriate allocation or low-cost trading of liabilities. Other aspects of trust enhancement may be provided by public or open, self-regulatory bodies. The sustainability of trust relationships in cyberspace markets may depend on asymmetry among the participants – in such cases, 'improvements' that reduce this asymmetry (such as the provision of identical information to both sides) may actually undermine trust.

If people choose trust in the face of 'exogenous' risks of loss due to accident or mistake, they can get locked-in to high or low trust behaviour independently of whether such behaviour is collectively efficient. If crime is added to the model, the rule of law may break down and criminal behaviour may become the prevailing practice. This depends on how people are connected: in fully-connected or symmetric situations, behaviour is likely to be homogeneous. Where networks are very asymmetric, a form of stable diversity is possible, with 'small worlds' or semi-private groups enjoying very different levels of trust.[203]

Trust may be viewed as a societal norm or convention. The stability of high trust behaviour does not depend on whether it is efficient, but rather on the balance of temptation and exposure. It may be that a population can be helped to evolve away from low trust lock-in at lower cost than that when an effort is made to force them into high trust equilibrium. The results are significantly different when crime is added to the picture – the policy interventions required to 'escape' the low

200 Katz and Shapiro 1994.

201 Anderson 2003; Cave 2004.

202 Cave 2004.

203 Cave 2004.

trust outcome may need to be both more extensive and more precise, and there is a danger of undermining the rule of law and getting locked-in to 'criminal equilibrium'.[204]

1.15 The Legislative and Policy Context – Privacy Protection

The evolution of the UK's crime prevention strategies will in part result from international cooperation. Some observers are concerned that the spread of global networks is outstripping the pace of law makers.[205] Although considerable international work is underway in this area, there are few signs that there will be efforts to adopt a formal international treaty.[206] This means that there is unlikely to be a clear international framework within which to consider the implications for crime prevention strategies for issues of privacy as cyberspace develops.

In the European Union a very high priority is being given to ensuring that Europe achieves competitiveness in the global knowledge-based economy. The Union's Lisbon strategy outlined policies, measures and actions that are expected to strengthen Europe's performance by accelerating the transition to the knowledge-based economy, 'while preserving – and modernising – Europe's unique social welfare model and decoupling economic growth from environmental damage'.[207] This intention to stimulate economic growth depends partly on leadership in the development and use of ICTs in ways that are both efficient and socially valued.

In some areas, such as technical standards and organisational practices to achieve improved risk management and crime reductions, the UK is well-placed to take the lead. It is argued by some that any measures (formal legislative or self-regulatory) that might discourage the early commercial introduction of advanced applications that have not been fully warranted for their dependability, could slow the pace of ICT innovation and dampen the competitiveness of the European information society. Others argue that it is essential to create economic incentives for cyber-technology suppliers and end-users to invest in greater levels of dependability and security even if this may slow the rate of diffusion of the most advanced technologies.

The parameters of the European Union's existing legislative framework that affects decisions about cyber trust and crime prevention are complex and involve numerous interdependencies. At the European Union level relevant legislation comes from directives on privacy and electronic communications, electronic commerce, telecommunication data protection, and consumer policy. As European legislation is transposed into legislation in the UK this, together with specific laws where the UK retains full national jurisdiction, creates a veritable jungle of legislation (see Appendix C for an illustrative list). These interactions can create contradictory outcomes because in some cases they foster greater privacy protection, while in others, they foster measures that alter the extent to which information about individuals is revealed for crime prevention purposes.

In the area of privacy protection, which has a major impact on the future deployment of cyberspace technologies, the opportunities for crime and the feasibility of certain crime prevention strategies, there are four broad classes of information privacy instruments (see Box 23 which excludes pressure-group activity, citizen and consumer education, market-based practices and contracts).[208]

---

204 Cave 2004.

205 Goodman, et al. 2002.

206 Bryen 2002.

207 European Commission 2003, p. 31.

208 Bennett and Raab 2003.

Box 23 Classes of Privacy Instruments

International Instruments – including the OECD guidelines on privacy, transborder data flows, information systems security and cryptography and the Convention of the Council of Europe 1981, and the European Union's Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of such Data, and the Electronic Communications Directive.

National Legislation – including national data protection laws, often overseen by privacy commissioners, as well as constitutional provisions (e.g., the Fourth Amendment in the US), privacy torts, contract-law remedies and privacy-protective restrictions in other laws (e.g., for the control of wiretapping). Comprehensive acts such as the UK's Data Protection Act 1998 and the supervisory body, the Office of the Information Commissioner, have emerged.

Self-regulation - a variety of 'voluntary' tools that include privacy commitments, codes of practice, adherence to standards, and online tokens or 'seals'. Self-regulation normally pertains to the private sector, although codes, commitments and the like appear in the public sector to cover practices such as video surveillance, online delivery of public services, etc. The 'Trust Charter' or 'Guarantee' proposed by the Government[209] to reassure the public about government data sharing is a UK example of the latter. The 'Safe Harbour' agreement between the US and the European Union in 2000 is an example of a self-regulatory initiative. Standards, such as ISO 17799 and BS 7799 also play an important role in information security and there is increasing attention being given to the need for a more general management standard. The development of privacy seals for the Internet environment includes schemes provided by TRUSTe (www.truste.org), the Better Business Bureau Online (www.bbbonline.org), and WebTrust (www.webstrust.org), but no scheme has achieved general recognition and credibility.

Privacy-Enhancing Technologies (PETs) **–** include systemic instruments (decisions of engineers who design networks, machinery or computer code, and technical standards and protocols); and collective instruments (such as public-key infrastructures for government service delivery and smart cards). Some PETs provide for individuals to make explicit choices about the privacy of their online transactions such as proprietary encryption instruments, devices for anonymity and pseudonymity, filtering instruments and privacy-management protocols such as the Platform for Privacy Preferences (P3P). The wide variety of available applications and their variable quality continues to militate against the use of PETs as a 'magic bullet' solving the privacy problem.[210]

The interdependence between the various instruments is not very well understood. In the UK, for example, the Information Commissioner has powers regarding the promotion and promulgation of codes of practice, and also contributes to policy- and statute-formation within government. The Information Commissioner's roles bring the Office into relationships with the media, pressure groups, technology designers and others whose activities affect privacy outcomes in a variety of ways. There is a growing need for a more holistic approach to regulatory policy and practice in the light of complex relationships and outcomes for privacy protection and crime prevention.[212] We examine the case of privacy protection and cyber trust to illustrate important ways in which policy developments in this area are likely to influence crime prevention strategies in the future.

Cyber Trust, Crime Prevention and Privacy Protection

The development of cyberspace including software agent-based computing and many knowledge management applications for cyberspace has drawn considerable attention to the need for protection against the privacy-invasive processing of personal information - 'For the general public

209 PIU 2002; DCA 2003.

210 Raab 2004.

211 Bennett and Raab 2003.

212 Bennett and Raab 2003.

as well as large swathes of the policy classes, … what baffles us often frightens us. What frightens us often stimulates, as well as feeds on, lack of trust in whatever it is that causes us to worry about our privacy'.[213] This observation is confirmed by studies of the public perception of risk (see section 4.1).

The underpinning of the *conventional privacy paradigm* rests on assumptions derived from liberal political philosophy and epistemology. Civil society is assumed to be comprised of relatively autonomous individuals who need a modicum of privacy in order to be able to fulfil the various roles of the citizen in a liberal democratic state.[214] Individuals are assumed to know their interests in privacy. Toward the end of the 19th century in the US, Warren and Brandeis defined privacy as 'the right to be let alone' and argued that 'the protection of society must come mainly through a recognition of the rights of the individual. Each man is responsible for his own acts and omissions only'.[215]

Surveys on privacy in many western countries suggest that people generally have high and increasing levels of concern about privacy.[216] Privacy is taken to be something that 'we' once had, but that is now being denied to us by public and private organisations employing the latest tools of cyberspace. As we have seen in section 4.1, popular culture and the mass media often amplify the public's concern. This conventional paradigm has encouraged the policy goal of giving individuals greater control of the information that is collected, stored, processed and disseminated about them by public, and in some cases, private organisations.[217] The paradigm and its assumptions underpin the doctrine of 'fair information principles' (FIPs) which has been codified in national data protection or information privacy laws, including the UK's Data Protection Act 1998, voluntary codes, and standards and guidelines. A notion of *balance* is a key feature of policy responses in this area because privacy must be balanced against other rights and obligations.[218] Critiques of this paradigm come from a number of perspectives as suggested in Box 24.

Because of its emphasis on procedural due process and on an individualistic construct of the value of privacy, it is difficult to raise distributional issues and equity concerns within the conventional privacy paradigm.[219] It is important to ascertain who enjoys what privacy, and why; and who does not, and whether an uneven distribution of data protection is justifiable on social and political grounds. The privacy paradigm does not address the distribution of privacy protection in terms of gender, ethnicity, social class, age, income, or other typical socio-economic and demographic categories.

213 Raab 2004.

214 Westin 1967.

215 Warren and Brandeis 1890, pp. 219-20.

216 Bennett and Raab 2004; Bennett 1992.

217 Laudon 1996; Lessig 1999; Raab 2003; Rule and Hunter 1999.

218 Raab 1999, 2004.

219 Raab 2004.

Box 24 Critiques of the Privacy Paradigm

Critiques of the privacy paradigm come from those who argue that the possessive-individualist implications of privacy should be rejected because this approach gives too little weight to community interests.[220] Some argue that this serves to legitimise personalised information systems and to extend social control in 'surveillance societies'.[221] The importance of privacy as a value for democratic society beyond the single individual or aggregate needs to be considered.[222]

A better understanding of the distributional characteristics of privacy protection would provide an evidence base for consideration of whether inequalities can be justified and whether public policy and its implementation can alter them. Privacy protection could be treated as an element of *social policy* and debated in terms of alternatives such as public or private provision, costs and benefits, responsibilities and entitlements, and the best way to 'deliver' privacy.[223] This issue is particularly important when we consider the way crime prevention is used to protect citizens from infringements to privacy and threats to their identities.

Existing data and privacy protection legislation aims to ensure consent for data storage, assurance that the data collected are necessary and that matching up of personal records, such as health and insurance records, with police data does not occur. However, the matching of information from different sources can be the basis for judgements about criminality. Despite assurances against the secondary use or linking of personal data, some people have little trust in those that currently and in the future will manage their data (see Box 25). [224]

Box 25 Identity and Identity Cards

Supporters of an identity card in the UK report that around 90 per cent of the population already carry identifying information on plastic cards and an ID card may prove more convenient enabling less cards to be carried. Card holders exercise 'informed consent' regarding their cards. However, combining information on one card gives rise to the potential for linking together different pieces of information about an individual's identity. This needs to be considered in the light of the fact that consent to reveal a 'piece of ourselves' in one context does not necessarily imply consent in another context.[225]

In addition, few of the most frequently used websites meet basic privacy standards.[226] Although cookies can be disabled, most people do not have the technical knowledge to do so and are unaware of firewalls and other protection mechanisms.[227] Many of the tools being developed for use in cyberspace such as encryption, digital signatures, digital pseudonyms and anonymous remailers are also available for criminals and terrorists. It may also be the case that too great a focus on limiting encryption may be at the expense more effective, yet less intrusive, crime prevention interventions. This may also apply to the excessive use of Closed Circuit Television (CCTV) surveillance as discussed in Box 26.

220 Allen 1985; Arndt 1949; Bolling 1996; Lyon 1994; Pateman 1983; Posner 1978.

221 Bowker and Star, 1999; Flaherty 1989; Gandy 1993; Lyon 2001; Marx 1988, 1999; Rule et al. 1980.

222 Raab 1997, 2004; Bennett and Raab 2003.

223 Bennett and Raab 2003; Raab 2004; Regan 1995; 2002; Schoeman 1992.

224 Rogerson and Pease 2003.

225 Rogerson and Pease 2003.

226 Electronic Privacy Information Centre 1997.

227 Rogerson and Pease 2003.

Box 26 CCTV Surveillance and Crime Prevention

Unimaginative implementation of CCTV may be contributing to concerns associated with the extension of its use. von Hirsch recommends that CCTV should be limited to the tracking of activity within a specific location over time, providing a record of activity for inspection when and only when an offence is known to have taken place.[228] Constant surveillance involves growing intrusion of privacy and the crime prevention benefits need to be sufficiently high to justify this and should directly benefit those being monitored. The effectiveness of CCTV as a crime prevention mechanism has not been empirically demonstrated.[229] The use of CCTV may lead to more self-policing as people aim to avoid being miss-recognised as criminals.[230] CCTV can be used to track individuals using human or software agents to identify faces, suspicious behaviour or a potentially criminal 'gait'. This raises issues of the ethics of crime prevention and whether class or other interests shape efforts designed to prevent crimes.[231] .

Ekblom argues that the goal should be to reduce crime to 'tolerable' levels,[232] while Kleinig suggests that a level of crime must be tolerated if it cannot be diminished without incurring unacceptable privacy intrusions.[233] Establishing what is 'unacceptable' is partly a matter for empirical research on citizen's beliefs and preferences, but it is also a matter for ethical debate. There are different interests and vantage points at to what constitutes 'acceptable' and 'unacceptable' levels of protection as suggested by the following:

> '…there is evidence that citizens are reacting to new anti-terrorism surveillance measures by calling for more checks and balances within their own democratic state structures. However, market agents are utilising new technologies to collect personal data, mostly in the absence of effective enforcement of privacy protection legislation, in order to financially benefit from their further processing and use'.[234]

Crime prevention to tackle crime linked to global networks in the future will rely on models that yield predictions and crime scenarios.[235] The perception of risk in cyberspace and of the acceptability of using intrusive technologies to monitor potentially criminal behaviour may become amplified or it may be attenuated depending on a wide variety of factors, many of which have come to light as a result of the review of existing scientific evidence. It seems clear, however, that much more will need to be done to ensure that cyberspace developments do not lead to the exacerbation of existing criminal opportunities or to new ones in the future.

This section illustrates that: 1. the economic dynamics of cyberspace markets tend towards horizontal and vertical integration with opportunities for lock-in to less than optimal systems; switching costs influence supplier and user incentives to invest in secure technologies; 2. the legislative and policy context for cyberspace is complicated by the need for cooperation at global, regional and national levels and by interdependence between policy instruments; 3. privacy protection would benefit from consideration in the light of social policy concerns about the equitable distribution of such protection; and 4. informed consent and anonymity are important issues in the use of identity cards and surveillance as means of crime prevention and, as yet, there is insufficient empirical evidence to back up claims about the effectiveness of these approaches.

228 von Hirsch 2000.

229 Welsh and Farrington 2002.

230 Palmer 2000.

231 Rogerson and Pease 2003.

232 Ekblom 1996.

233 Kleinig 2001.

234 Institute for Prospective Technological Studies 2003, p. 19.

235 Levi 2001.

7 CYBER TRUST AND CRIME PREVENTION - KEY ISSUES AND LESSONS

In this section, we draw upon the preceding sections to provide a review of the key issues and lessons from the scientific evidence. We highlight especially those areas where there is a need for measures to encourage the development of trustworthy cyberspace systems and improved strategies for crime prevention. In most cases, such measures will need to be underpinned by a stronger cross-disciplinary research effort.

The preceding sections offer many insights into the interrelationships between the human and technical components of cyberspace. These need to be distilled to highlight areas where there are gaps in understanding and where there is consensus or controversy about future developments. We have stressed that cyberspace is a complex human and technical system. This observation is increasingly widely accepted by experts and non-experts alike. What is much less well understood by stakeholders, including cyberspace system developers and users, is that *the whole of this system is subject to unpredictable emergent behaviour, which may yield unintended results*. This means that the balance between the anticipation of, and scanning for, new problems leading to reactions is likely to favour the latter. More will need to be invested in scanning for new forms of criminal activity, enabling versatile responses and ensuring that, in cases where remedies fail, there is sufficient redundancy in the system.

This means that at any given time, parts of the system will be relatively stable while other parts are unstable.[236] It also means that there will always be ambiguity in the interpretation of the results of research. This is because the co-evolution of all the components of cyberspace is subject to a large number of possible emergent outcomes. This observation has particular consequences for interventions aimed at improved crime prevention because interventions for other purposes may confound crime prevention. Nevertheless, there is sufficient evidence from existing studies of cyberspace developments, and more generally, from research in related areas of science and technology, to draw inferences about the outcomes associated with the most likely future developments. In the face of uncertainty and the need to strengthen the evidence base in key areas, decisions about the most effective crime prevention strategies must be considered in the light of ethical considerations and principles that are derived from plausible theories.

The existing scientific evidence can be applied to clarify some of the interdependencies between the human and technical components of cyberspace, especially in areas that have achieved a degree of stability. This helps to suggest how interventions in cyberspace are likely to reverberate throughout the whole social and technical system, locally and globally. Our review of developments in cyberspace technologies and components of the social system demonstrates that – in nearly every area - there are new opportunities for criminal activity. Strategies to mitigate these involve numerous trade-offs and choices, some of which we consider in this section.

In section 2.0 ('Scope and Salience of the Issues') we highlighted the fact that as the dynamics of the cyberspace system unfold much will need to be done to build confidence both in people and in the 'mechanics' of cyberspace. As electronic services continue to evolve, people will appraise cyberspace threats in different ways and give them quite different meanings. The variety of responses will depend on the way different people value the consequences of perceived threats. This means that a better understanding of the relationships between human factors, risk and trust is essential for the future security of cyberspace.

236 The OST Foresight programme has been examining complex systems within the framework of the Foresight Cognitive Systems Project, see Austin et al. 2003 for review.

So far, relatively little attention has been given to the analysis of public perceptions of cyberspace risk. This is a major gap in the evidence base.[237] We can infer, however, from studies of the public perception of risk in other fields of science and technology that there is a complex set of risk factors. This research indicates that future problems and perceived dangers in cyberspace could be interpreted by the public as a failure of the technical system, as a failure of the system designers and users, or as a failure of the perceived governance model. It is also essential to bear in mind that reported perceptions of risk may not be aligned with the trust that people actually place in cyberspace technologies or in the individuals (and software agents) and institutions that govern cyberspace.

It is clear from research undertaken by organisations across Europe that the solutions for improving cyber trust and crime prevention in a pervasive computing environment will be quite different from those in use today. There will be a need for *a new paradigm for cyberspace security*, even in the face of the current situation in which majority of potential users of cyberspace services and products have a poor understanding of security.[238]

In section 2 of this report, we posed several questions:

- What sorts of cyber trust issues will be of dominant concern – what will be the new kinds of vulnerability and how will the risks of cyberspace be perceived?
- How will the overall structure of the emerging system drive the uptake of cyber trust technologies?
- What kinds of interventions might be made to influence the system's dynamics for the purpose of improving cyber trust and crime prevention?

Some answers are provided in the discussion that follows, but it is important to remember that addressing these questions within existing paradigms of trust, security and technology is unlikely to be enough to alleviate concerns about potential threats in this environment. A strengthened cross-disciplinary research effort is needed to create a better foundation for understanding key facets of the technical and human dimensions of cyberspace.

1.16 Dependable Software Systems and Commercial Issues

We have considered the dependability of pervasive and complex computing systems and the development of various means of identity verification and authentication of users of these systems (section 3.0 'Constructing and Using Cyberspace Systems'). A *deployment gap* is associated with software development methods and procedures. These are currently insufficiently robust to produce a more trustworthy network infrastructure and service applications. The dependability or 'trustworthiness' of a computer system refers to the ability to avoid computer system failures beyond an 'acceptable' level.

One key issue is *the level of failure* that would be regarded by users as being unacceptable.[239] Another is the *management* of the software engineering process in which there are numerous dependencies and constraints. In response to the first issue, there is a need to develop fault prevention and fault removal techniques that maintain satisfactory service in the face of attacks on networks. In response to the second, there is a need for good project leadership and close

237 OST Foresight in commissioning research reviews in this area. There is some research on perceptions of risk with respect to the Y2K issue (Pidgeon et al. 2003) and on risk management particularly in the financial services sector (Backhouse 2003).

238 See section 2.0.

239 Jones and Randell 2004.

involvement of the customer to ensure that the system meets required levels of dependability, and standards against which system dependability performance can be measured.

In large-scale software engineering projects there is a need to capture user requirements in a systematic way and for flexibility in the development process in order to respond to changes in the external environment. This means that it is essential to use educated and experienced people in the design and implementation of large software projects in order to minimise the risk of unacceptably low levels of system dependability. If future networked computer systems are to attain improved levels of dependability or trustworthiness, considerably greater attention will need to be given both to commercial issues that influence customer willingness to invest in such systems and issues of risk management. Improved methods of managing the components of large-scale software projects will be needed. Regardless of whether components of large-scale software projects are developed using proprietary or open source software code, and whether they rely on re-usable code, the problems of managing the component aggregation/disaggregation process will remain.

It may become technically feasible to develop *warrantable* software and systems. This would require a software system development approach that: 1) enables the likely impact on system dependability of all design and deployment decisions and activities to be assessed throughout the system life cycle, and 2) caters for system adaptation and the realities of huge, rapidly evolving, pervasive systems.[240]

In this context, the commercial relationship between those who commission a project and the developers and deliverers of a project involves financial, functional and time risks, all of which need to be managed in an equitable manner. Contracting regimes may be based on fixed price or cost plus arrangements, but because of the difficulties of estimation and resource allocation and unexpected component integration problems, adherence to a rigid structure of contracting regimes often contributes to the failure of such projects. 'Best practice' codes can play a role, but adjustments and flexibility are needed together with the skills of a change manager with a very high level of expertise, experience and education.

Incentives for all parties involved in complex software projects to adopt 'best practice' are essential as is the maintenance of an intimate collaborative relationship on all aspects of a software project.[241] In addition to the methods for managing technical, financial and timescale risks, software development involves two additional risks. *The first involves estimation*. The lack of any physical law constraints causes considerable uncertainty as to how long a piece of software will take to develop.

To address this risk there is a need to achieve a balance between delivering functionality within the expected time and cost while not bounding the creativity of the software developer to deliver functional code. At present software development is seen as a mixture of an art and science. The challenge for software engineers in attempting to provide solutions to large complex problems is that the complexity of the solution itself is poorly understood. In addition, the processes by which such complex artefacts are created are complex and ill-defined. Concentration on the modularity of functionality is leading to neglect of the connectivity between the software modules (see Box 27).[242]

240 Jones and Randell 2004.

241 Collins 2004.

242 Collins 2004.

Box 27 A Holistic View of Modularity

A holistic view of modularity and the links between modules is essential if the implicit decomposition that modularity implies is to be successful. Other engineering disciplines adopt holistic approaches to the design of large complex structures. The context of software engineering is no different. While there are no physical laws and the constraints are less rigorous and well-shared within the project, it might be beneficial to the software engineering community if the approaches that are taken to holistic engineering in other disciplines are evaluated for their applicability in the software engineering process. [243]

The *second specific risk* that is encountered in large-scale software projects is the difficulty of describing accurately the relationship between the critical elements of the requirements. The use of prototyping, rapid application development approaches, or other approaches to risk reduction on critical uncertainties within a project, can help to mitigate this risk. It is mainly people who write software. There is research on how software could be used to generate software, but automatic software generation tools have been used with little widespread success. For the foreseeable future, people will continue to play a critical role in the generation of software. Greater efforts are needed to encourage a holistic view of software engineering in order to reduce the risks of software unreliability. In addition, there are divergent views about whether the open source software movement can produce software that attains greater reliability and dependability when it is used on a large scale and as components of hybrid proprietary/open source applications.

Achieving greater dependability of complex ICT systems in the future will require greater investment in training and education. On a global scale education in software engineering and computer science is increasing, but in the UK it is on the wane. Efforts to improve this situation are being made by a number of bodies, but the skills and expertise available to British industry in this field are declining. The key issue is appropriate education to produce graduates that are capable of participating effectively in the development of large complex software projects.[244] The skills base necessary to develop trustworthy software requires experienced professionals that are appropriately certified or chartered. It also requires that employers need to recognise that it is imperative that they recruit experienced people to work on projects to develop software. To ensure that such people are available the overall qualifications of the labour pool must be continuously upgraded. Also there must be greater awareness of vulnerabilities among those who invest in the components of cyberspace systems. This would create stronger incentives to introduce measures aimed at reducing cyberspace system vulnerabilities.

Future research on the dependability of software systems must be cross-disciplinary. It will need to bring together those who undertake research within technical and procedural disciplines that presently concentrate on particular types of systems, dependability attributes, types of faults, and means for achieving dependability, with researchers who tackle socio-technical issues including design, usability, functionality specification, acceptable levels of failure, recovery modes and incident management as well as ‘best practices’, and innovative approaches to project management and software engineering throughout the whole of the life cycle. If the practice of software engineering is strengthened by measures that enhance the dependability or trustworthiness of software systems the opportunities for criminal attack or accidental failure could be minimised.

The UK could gain a competitive advantage if it provides leadership in standards setting with respect to the testing and certification of all aspects of dependable systems, including autonomous software agents. If processes and systems created in the UK are accredited, and this accreditation is seen elsewhere as having value, practices, procedures and technical designs, especially with

243 Collins 2004.

244 Collins 2004.

respect to networks and software, could spread rapidly as a result of externalities with a strong potential for global impact. However, for this to happen cyberspace systems developers and users would need to see a financial return, given the additional costs of more dependable systems. This suggests the need for cross-disciplinary research on the economic incentives that will arise in future markets and the links between these incentives, people's perceptions of risk and their willingness to trust networks despite their relatively low levels of dependability (economic incentives and markets are considered below in section 7.7).

1.17 Managing Identity(ies) in Cyberspace

One of the most significant issues for crime prevention is the fact that in cyberspace users may choose to maintain their anonymity. In addition, new identification issues will be raised in areas where identification of users is essential for commercial services, or for access, for instance, to health records and income tax returns or for crime prevention, for example, the appropriate means of authentication of identity. In section 3.3 ('Identification and Authentication in Cyberspace'), we examined the many instances in which people, devices or digital data need to be identified and authenticated. Users (including computers, software agents and people) can be authenticated using something they own, something they know, or something they are. All these techniques, whether used alone or in combination, assume that there has been an initial, accurate identification and then rely on that assumption. If the original identification is not conducted properly then there is a risk of error in later identification.

Passwords, encryption and biometrics can be used as means of identification. The last offers a direct means of authentication but, even in this case, there is a risk of error insofar as no two biometric templates match perfectly. When a decision is made a Type 1 error may occur such that the system fails to recognise a valid user or a Type 2 error may occur and the system accepts an impostor. The likelihood of such errors has implications for the usability of cyberspace systems and for the extent of actual and perceived risk. Decisions in this area will influence the perceived trustworthiness of service applications that are supported by the cyberspace infrastructure and raise questions about people's attitudes to intrusions into their bodies.[245] One means of addressing this area will be to examine empirically how people respond to specific measures and how they perceive the trade-offs between intrusions and protection, and their respective benefits and costs. Use of biometrics will mean that it will not be possible to maintain multiple core identities for a given purpose without introducing considerable system and process complexity.

1.18 Cyberspace Usability, Risk Management and Security

Changes in the design of secure technologies and in social practices and cultural norms of information assurance influence the effectiveness of strategies to reduce crime and threats arising from changes in information handling procedures. Empirical research demonstrates that, despite the availability of mechanisms that can be used to authenticate the identity of cyberspace users, many of these are hard to use or are rendered ineffective because of the demands they make on users. Unless users are given training in the use of those mechanisms that are available, human error will make them of little benefit.

The usability of such mechanisms as passwords, tokens and encryption, depends on the organisational processes and the workflows that are involved as well as on the extent to which users believe themselves to be at risk. Studies of organisational and behavioural change demonstrate that effective risk management requires the development of a 'culture of security' where end-users, rather than their physically present or distant managers, take responsibility for monitoring risks and acting appropriately. Although codes of information security management

245 It should be noted that biometric solutions using iris recognition that do not rely upon the use of a data template are being developed. If the method is scalable, and the signs are encouraging, this has potential. However, usability studies show that there will be a small percentage of the population for whom this will not be feasible (see section 3.3.2).

have been developed, the complexity of cyberspace systems and the danger of unwanted intrusion or attack mean that there will be an increasing need for the interoperation of management policies and new frameworks to ensure that security measures become more closely integrated into business processes. In parallel with the need for new approaches to software engineering and the design of large complex software systems, there is a need to foster *persuasive design techniques* that reward cyberspace users for good security practices.

A key lesson from empirical research on security mechanisms and behaviours is that appropriate and effective security must be an integral part of the socio-technical system. Security needs to be integrated into all cyberspace development approaches. A central focus for crime prevention strategies may be the point at which human beings directly interface with the digital world. Research on cyberspace market evolution also suggests that as the cyberspace system evolves, a major area of development concerns the technical interfaces and standards that are used. These interfaces and standards are the vulnerable points in cyberspace in terms of security and the risks associated with them will either be amplified or attenuated in the future.

The vast scale and scope of cyberspace also highlights the need to achieve greater reliability in the authentication of information and digital documentation, which may be accompanied by meta-data describing a document's use and functionality. This raises issues of digital rights management, data and information ownership, identity, and privacy.[246] As agent software is used in an increasingly large number of cyberspace applications, the necessity for identification and authentication of software and data objects, as well as people, will grow.

There will continue to be a need for research into the security of technology and on the effectiveness of identification processes used for important everyday processes. The questions that will need to be addressed on an ongoing basis are: 1) how much 'security' or 'strength' is appropriate? 2) What is the appropriate balance between procedural approaches and architectural solutions to reduce the risk of vulnerabilities arising as a result of human behaviour? 3) What kinds of education programmes could be used to highlight the need for compliance with local security policies?[247]

1.19 Cyberspace and Crime Prevention Strategies

Crime occurs in many forms and one way of describing generic crime problems and solutions as a guide to future crime prevention strategies for cyberspace is the Misdeeds and Security framework. This is shown in Table 6 which could be modified as further consideration is given to the risks encountered in cyberspace.

246 This issue is examined in section 7.7.

247 The European Commission has launched a 'preparatory action', 'Towards a programme to advance European security through Research and Technology', IP/04/145, Brussels, 5 Feb 04. The programme covers improving situation awareness; optimising security and protection of networked systems; protecting against terrorism; enhancing crisis management; and achieving interoperability and integrated systems for information and communication.

Table 6 Cyberspace Developments at Risk and Security Measures

Misdeeds (Ms)	Actions Supporting Security (Ss)
Misappropriated (theft)	Secured against theft
Mistreated (damaged or injured)	Safeguarded against damage
Misused (for crime, including counter measures against prevention or enforcement)	Shielded against misuse
Mishandled (fraud, counterfeiting, smuggling, illegal divulgence)	Supporting – justice, crime reduction, community safety (facilitating arrest, forensics, identification, punishment, reassurance)
Misbehaved (disorder and antisocial behaviour)	Scam-proofed
Mistaken (false alarms, wrongful accusation, leading to miscarriage)	'Sivilized' –conducive to good behaviour
Mistrusted (non-reporting of crime to authorities)	Straightening adverse side-effects

Source: Adapted from Ekblom (2004a).

Cyberspace developments of this kind could be addressed in the context of crime prevention strategies through the further elaboration of *criminal opportunity models*. Felson's routine activity theory has been used to encourage those responsible for crime prevention to consider the physical and virtual locations and times in everyday life when motivated offenders are likely to become motivated by contact with vulnerable crime targets, especially in the absence of 'capable guardians'.[248] In an extension of this model, efforts are being made to develop crime prevention activities to reduce the likelihood of the 'conjunction of criminal opportunity'.[249]

The 'conjunction of criminal opportunity' model provides a means of systematically considering the conditions necessary for a crime to occur and the possibilities for prevention. It focuses both on the predispositions of potential offenders and on the immediate characteristics of the crime situation – in this case the online and offline situation of cyberspace users and the systems within which they operate.[250] With respect to the situation, the model signposts many factors that encourage crime. Crime prevention can be defined as an intervention that tackles the causes of criminal events to reduce the risk of their occurrence and/or the potential seriousness of their consequences. The causes of crime can be complex, but also remote and fairly weak. However, immediate causes are reducible to 11 generic precursors which act through common aspects of crime situations and of criminals – whether in the physical world or in cyberspace.

The conjunction of criminal opportunity occurs when a predisposed, motivated and equipped offender encounters, seeks or engineers a crime situation involving human, material or informational targets, enclosures (such as a building or a firewall), a wider environment (such as a shopping centre or a financial system) and people (or intelligent software agents), which are acting in diverse ways as crime preventers or promoters (see Table 7).

Preventive interventions can act by interrupting, diverting or weakening any of these causes. Understanding these resources for offending is important because they influence the situation that

248 Felson 1987.

249 Ekblom 2003; Rogerson and Pease 2003.

250 Ekblom, 2002, 2003.

crime preventers confront and the strength of the offender's predisposition and motivation to commit a crime (Ekblom and Tilley 2000).

Table 7 Generic Precursors of Crime

Potential Offender	Crime Situation
Presence (incl. virtual) in crime situation without leaving traces	Target of crime (person, company, govt.; material goods, systems, information) that is vulnerable, attractive or provocative
Perception of risk, effort, reward and conscience and consequent decisions	Enclosure (safe, building, firewall) that is vulnerable, contains targets
Resources for crime (skills, weapons, knowledge, equipment, access to supporting network; *modus operandi* to maximize reward and minimize risk and effort, creating a crime opportunity.	Wider environment (town centre, airport, computerized financial system) that contains targets, generates conflict; favours concealment, ambush and escape over surveillance and pursuit
Readiness to offend (motivation, emotion, influenced by current life circumstances)	Absence of preventers (people or intelligent software) that make crimes less likely to happen
Lack of skills to avoid committing crime (literacy, social skills)	Presence of promoters (people or intelligent software) that make crime more likely to happen, including careless individuals, reckless designers/manufacturers, deliberate fences and criminal service providers
Predisposition to criminality (personality, ideology)	

Source: Ekblom (2004b).

Trust fits into this framework in several ways. An Internet shopper who is too trusting may act as a careless or negligent crime promoter, as may a system designer. Conversely, being an effective crime preventer means being equipped with appropriate applications and systems. Offenders exploit misplaced trust, sometimes to an expert degree and are aided by software and hardware based resources, for example, 'skimming' devices fitted into cash machines to clone cards.

Efforts to improve the security of complex information systems often rely on the use of risk analysis to justify the cost of designing and implementing security features.[251] The concept of a *criminal opportunity* can be used to understand the means of reducing crime opportunities in organisational contexts where threats to security are posed by dishonest staff.[252] Clarke's 'Crime Specific Opportunity Structure' model focuses, for example, on the opportunities available to potential inside perpetrators of network related crimes.[253]

These approaches could be extended to examine the organisational contexts and behavioural characteristics that are most likely to give rise to criminal opportunities. Notwithstanding the development of these approaches, answers to questions about the acceptable levels of the dependability and trade-offs require an understanding of the nature of trusting behaviour among human and software agents and of the actual and perceived risk associated with cyberspace.

A key area is this context is *ICT Forensics.* Data held on hard disks can be put to criminal use. If they can be identified and authenticated, these data can provide evidence of malfeasance. The problem of identifying 'the original' is difficult and frequently overlooked. In the future, as the scale

251 Courtney 1977; Fitzgerald 1978.

252 Backhouse et al. 2004; BloomBecker 1984; Forester and Morrison 1994; Hitchings 1995; Willison 2002.

253 Clarke 1995, 1997; Clarke and Cornish 1985; Cornish and Clarke 1986; Clarke and Cornish 2000; Brantingham and Brantingham 1991; Hirschi 1969; Felson 1992; Hindelang, et al. 1978.

of cyberspace systems increases, the sheer volume of distributed stored data may overwhelm the capacity of law enforcement agencies. Even as data management tools are developed, they are not likely to have the processes of auditability and traceability incorporated in them required for evidence gathering. It will be necessary, therefore, to document these requirements, which, in turn, will require stakeholder collaboration to agree the principles and standards to be met.[254].

As data are increasingly likely to be stored in jurisdictions beyond the reach of national law enforcement agencies some form of international code of practice will be needed to enable access to data by agencies involved in crime detection and criminal prosecutions. If the match between these data and a suspect with seemingly appropriate spatial and temporal proof is insufficiently strong, the data will not stand up in court as evidence. One objective in using forensic data could be to establish sufficient strength of 'binding' or linkage to allow other physical investigations to be instigated that would add to this evidence. This would require collaboration between system designers and legal and law enforcement specialists.

The availability of mobile and transportable miniature mass storage devices that use strong encryption will expand enormously over the next decade. Reliance on the analysis of log files to identify when and where specific devices have accessed or are accessing systems and networks and being able to very rapidly and accurately trace subsequent use seems the only means at present for tracing illegal activities. As the volume of encrypted material within which the criminal can conceal his or her activities increases, it is possible that, where data are shown to be encrypted and not legitimate, they could be used to justify further investigations. The question of whether the public or private sector would be willing to bear the costs of very expensive tracking or endure rapidly spreading and unprosecutable crime, is an urgent subject for debate.

Forensic tools are being developed by a very small number of academic groups and companies to meet specific needs. Without some collaboration with their developers, the ability of investigators and computer forensic experts to maintain parity with the environment within which the data under investigation are used and stored, will be limited. The ability to carry out forensic investigations will need to be seen as a legitimate requirement placed on a system or application design if this situation is not to become worse. All of these issues need discussion, but it is unclear who should initiate it. There is some indication that cyberspace users do not 'want to know' in advance of any potential weaknesses. Nevertheless, there is a need to consider what balance between evidential – investigative – preventative computer forensics could be struck and the risks and benefits of the various options.

At present there has been little fundamental research into the issues of the scale of cyberspace and the criminal use of data, especially that stored outside the jurisdictions of law enforcement agencies, and the ethical, social, economic and legal strategies that might be adopted. There is a need for cross-disciplinary research in the area of ICT forensics and cyber-evidence management. Enhancement of trustworthiness itself will reduce the likelihood of malfeasance by temptation, but without strong cyber-policing, the determined criminal will find in the use of ICTs and the applications that will be running on the Internet, a 'honey pot' of opportunity and illegal gain.

1.20 Trust and Risk in Cyberspace

We examined research on risk perception and on trust in section 4.0. There is a growing body of literature that provides insight into whether the technical possibility of risk in cyberspace is the same as the perception and actual experience of risk. We can gain insight into perceptions of risk in cyberspace by drawing upon research into the way members of the public have been found to appraise uncertainty and the risks associated with scientific and technological innovations. It

254 See section 7.7 on new digital principles.

seems clear that the social meaning of a risk will influence its salience and the way uncertainty is judged. People's perceptions of risk are related to their cultural and social values, their attitudes to blame, their morality and how they view an event such as an intrusion that reveals their identity in cyberspace. In addition, the attitude of the public towards experts and regulators can be expected to influence the way cyberspace risks are interpreted. Risk perception is also intimately linked to levels of trust.

These observations rely on theories and empirical research in the fields of cognitive psychology, psychometric analysis and studies of risk and emotion. There is also evidence from studies in the field of media and communications that people's perceptions of risk are strongly influenced by the symbols within their social networks and in the media's reporting of events. There is empirical evidence based on people's stories about their perceptions of risk that suggests that whereas experts see risks as chains of cause and event, lay people tend to see them in a social context of relationships. Research is needed to assess the importance of these observations for cyberspace and crime prevention. This body of research helps to explain why probabilistic analyses of actual risk may vary considerably from analyses that take the context of cyberspace experience into account in a qualitative way.

It is also important to distinguish between reported perceptions of trust and the way in which people actually conduct their lives. We have little evidence of the extent of inconsistency between reports of mistrust in individuals or institutions and the capacity to place trust in various parts of the socio-technical system.[255]

The literature on risk perception suggests that perceived risk may be amplified or attenuated depending on a large number of socio-technical factors. The Social Amplification of Risk Framework (SARF) has been developed as a means of integrating disparate approaches to risk.[256] The SARF:

> '… aims to examine broadly, and in social and historical context, how risk and risk events interact with psychology, social, institutional, and cultural processes in ways that amplify and attenuate risk perceptions and concerns, and thereby shape risk behavior, influence institutional processes, and affect risk consequences'.[257]

Debates among adherents to different positions with regard to the risk people will encounter or perceive in cyberspace are informed by very different knowledge claims.[258] The SARF could be further developed to understand why some risks associated with cyberspace attract heightened social and political attention (risk amplification), even when experts judge them to be relatively unimportant. Application of the SARF could provide a framework for evaluating the likely effectiveness of crime prevention strategies.

We know that trust is a means for alleviating risks, but there is little empirical research on the conditions under which people are prepared to trust others in cyberspace or to trust in the trustworthiness of cyberspace systems. Yet with the spread of access to global networks, it is clear that in many circumstances people are willing to trust in each other, in the cyberspace system, and in the notion that system-to-system interdependencies and relationships are sufficiently trustworthy. Empirical research in the fields of human-computer interaction and computer-mediated communication is beginning to provide insight into person-to-person and person-to-system trust in

255 O'Neil 2002.

256 Jackson et al. 2004; Kasperson et al. 1988; 2003.

257 Pidgeon et al. 2003, p. 2.

258 Callon 2003; Rosa 2003.

cyberspace. Key variables influencing trust include: the number of actors involved, the types of actors, whether relationships are conducted synchronously or asynchronously, the availability of trust-warranting properties and signals to convey those properties, prior experience and the propensity to trust, and the perceived benefits and risk of trusting behaviour.

It seems that as more information exchanges are mediated by technology, the responsibility for supporting trust will increasingly fall on cyberspace system designers and operators. Studies of trusting behaviour in these areas also provide suggestions for the types of factors that are likely to influence agent-based behaviour in contexts where system-to-system trust must be established. However, most of the research in this area is conducted using stylised game-theoretic models, which limit the number of variables that can be examined in a given 'game' as discussed below, and are difficult to populate with data reflecting the experiences of cyberspace users.

Empirical evidence suggests that the propensity to trust another person or software agent is partly informed by expectations. Agents' expectations also can be modelled probabilistically to provide insight into the likelihood that choices about whether or not to trust will yield various outcomes. Such game-theoretic approaches assume that an agent's decision to play in a game involves trust that actor(s) will behave as expected. The outcomes of the games are influenced by the completeness of the institutional framework (laws, rules, and standards), by completeness of information available to the agents in the game, and the network structure of the game that is established at the outset.

One application of this approach is a coordination game in which it is feasible to establish whether high or low trust equilibria will emerge if all the agents interact in a fully connected network according to a pre-specified set of rules and definitions of trustworthiness. One of the assumptions in this approach is that the players engaged in a game will act rationally and this allows their behaviour to be predicted. This approach facilitates understanding of the consequences of precautions that may be taken to avoid crime in the face of externalities. Research in this area helps to demonstrate when such measures are likely to affect risk to others and when it is appropriate to transfer the cost of protection to others, i.e. from the cyberspace system developer to the end-user firm or the consumer. This work suggests that *it is the distribution, rather than the level, of trust* that supports the setting of priorities for establishing trust relationships and establishes a structure for negotiating the distribution of liabilities arising from cyberspace interactions.

In recent years there has been a revival of the concept of social capital in which trust is a major component. This concept can be applied to examine the positive effects expected from networks of trusted agents. Drawn from studies in sociology, human geography and economics, it has been suggested that societies with a more complex and dense pattern of networked social relations may benefit from lower transaction costs and stronger assumptions about whether agents will act opportunistically. This approach could be extended in the future to examinations of the way webs or networks of trust emerge in virtual communities of various kinds. There is a need to better understand how social capital can be fostered in cyberspace.

Just as there is uncertainty about how best to design and operate trustworthy or dependable cyberspace systems, the trusting behaviour and trustworthiness of human and software agents is not clearly understood. In the light of this uncertainty, it is important to consider cyber trust and crime prevention issues in terms of the ethical issues, especially with respect to identity, anonymity and privacy. In cases where the evidence-base is weak, we also need to rely on principles derived from plausible theories. We have seen that cyberspace security systems often require identity authentication, but the Internet is currently designed to facilitate the way people can 'play' with their

identity. This will remain the case, as long as the design and architecture of the Internet provides for anonymous communications.[259]

Views are divided about the ethical justification for interventions in cyberspace that seek to limit this potential. From an ethical standpoint, this suggests the need for a forum in which those who remain sceptical of the need for security interventions to prevent crime indicate their requirement for justification of changes that might limit the scope for anonymity. However, in sections 4.1 and 4.4 of this report, we have discussed why it is so difficult to discuss these key issues in generic open forums. The principal difficulties are the extent to which different meanings become attached to the perceptions of risk and danger, uncertainty about how the media are likely to influence opinion in this area, and the strongly polarised views about the origins and appropriate future of the Internet.

With respect to the polarised views about the Internet, while some seek to place the burden of proof on those who wish to alter the libertarian and open principles that underpin the Internet as we know it today, others argue that, although recognising that certain privileged activities such as science or commerce must be able to continue in a secure way, liberty and openness are important values. The judgements could, however, be made by those with political power, in which case the trade-offs between individual privacy and the benefits of greater collective security would need to be taken into account in a way that specific issues would be considered and assessed as transparently as possible.[260]

From an ethical standpoint, some regard trust as the effect of good behaviour while others regard it as being the cause of good behaviour. Some argue that liberty and openness are essential and non-negotiable in cyberspace; others want to alter the design of cyberspace to make inappropriate behaviour more difficult. Different views about the moral arguments supporting different approaches to crime prevention strategies for cyberspace hinge on the extent to which actors are presumed to be rational and are likely to act to maximise their own self-interest. In an environment where there are multiple complete or partial identities, standard assumptions about what motivates actors need, at the very least, to be carefully scrutinised.

Having originated in the west, the Internet has a western bias, which tends to inform debates and policies for crime prevention. On the one hand, it can be argued that actors should be allowed to pursue their conception of the ‘good’ (if this does not interfere with others). On the other hand, it can be argued that there should be no departure from western principles and their implications for crime or cyber-terrorism. It is also possible, however, to argue that the key issue is the privileges that people should have in cyberspace, thus enabling debate about this to become a political problem that may be addressed through compromise and various *social policy measures.*

Positions on this issue are closely linked to the role of the media and strategies for building awareness of the risks in cyberspace and about trust and the trustworthiness of cyberspace. As with other issues where there is uncertainty and a possibility of the amplification of risk, if there is to be informed and reasoned debate about these issues, citizens must be well informed about cyber trust and crime prevention issues.

---

[259] Since the Internet and its platforms are subject to continuous evolution, it is important to distinguish analytically here between the public and private spaces that can be created, the changes in the Internet Protocol with respect to quality of service and other features, and the differences in the requirements for security of various industry sectors, government services, and public spaces frequented by citizens and civil society groups.

260 Issues of privacy and the potential trade-offs are considered in section 7.7.

The government, the private sector, citizens and civil society groups - as well as the traditional and alternative media outlets – will continue to draw attention to many of the problems and issues in this area.[261] The debates that ensue will not all be based on reasoned argument and the provenance of some information upon which these debates rely may be difficult or impossible to trace. However, as awareness of cyberspace risk and vulnerability continues to spread, there are growing numbers of forums (nationally and internationally) that are seeking to foster critical and reasoned debate and measures to tackle specific issues. This highlights the importance of ongoing monitoring by governments and other actors of opportunities to facilitate such debates such that consideration is given to the feasibility and appropriateness of actions proposed to limit crime.

Existing theory and empirical evidence do not support unambiguous conclusions in this area. This is to be expected given the emergent properties of a complex system. Similarly, there are a substantial number of models and perspectives on trust and trustworthiness in cyberspace, but these enable relatively few inferences to be drawn about trust and trustworthiness. One of the difficulties of translating the results of existing research into practical solutions for crime prevention is that many conceptual frameworks and models are based on strict parameters and assumptions and some approaches do not lend themselves to empirical verification.

Those that can be analysed empirically often yield results that are open to different interpretations depending on views about how opinions are influenced by the media and other psychological and sociological factors. In addition, even though the use of computers and the Internet has reached a reasonably high level in the UK, the more advanced components of cyberspace systems have yet to diffuse widely. Globally, too, usage is vary uneven and interactions are globally dispersed in many cases adding to the difficulties involved in understanding trust and risk perception. This too is an area that represents a major gap in the evidence base necessary to support more effective crime prevention strategies.

1.21 New Cyberspace Technologies and Trust

We have examined how various models of trust are being applied in two important areas of technical development – software agent-based systems and knowledge technologies and the semantic web (section 5.0 above).

If cyberspace systems are to become more dependable and secure there will need to be changes in the design and implementation of the ICT components. Agent-based computing is regarded as a means of achieving this. Software agents have to trust each other in order to minimise the uncertainty associated with their interactions and take account of individual and system-level trust. In both cases, there is a need for protocols that ensure that the software and human agents will find no better option than telling the truth and interacting honestly with each other. This is a major challenge for the future.

In addition, new knowledge technologies and work on the semantic web require requires a certain degree of trust in the means of ensuring that the input to knowledge and information manipulation processes are trustworthy. The available tactics for imbuing trust include transparency, ownership rules, the means to extend trust between sub-networks, certification, restrictions on entry, formal methods, calculations, interrogation and knowledge management. Research in this area shows that each of these tactics has costs and benefits and that they must be combined with effective trust management strategies for the software systems – including the use of metadata and

261 There are growing numbers of articles in the press focusing, for instance, on the impact of anti-spam laws in the US, use of software for anti-terrorism surveillance, and the privacy and freedom of speech issues that are raised. The future issues raised by this report indicate that information control and assurance, together with the overall stability of the cyberspace system will continue to provide a focus for, and give rise to, debate.

ontologies for trust requirements. All of these tactics raise questions with respect to identity, anonymity and privacy.

Effective procedures for the maintenance of knowledge bases will need to be developed to ensure that, as sharing of knowledge in a controlled way becomes a major influence on commercial and social behaviour, the sources used are maintained and exploited in ways that ensure they can be trusted. At present there is very little understanding of the end-user's perspective on these issues.

A problem related to research aimed at examining end-user perceptions of trust and the trustworthiness of cyberspace is that it is difficult to define trust in a way that is meaningful for survey respondents. When trust is defined as a 'confident expectation', survey results for the UK suggest that the relationship between information about the Internet, uncertainty and trust varies along many dimensions, including the extent of experience in using online forms of communication.[262] Trust appears to be enhanced as a person learns more about the technology, but experience over time may also create new uncertainties and perceptions of risk. Individuals with more formal education tend to be somewhat more sceptical of the information and people accessible on the Internet, but also somewhat less concerned about the risks of Internet use. Evidence and analysis are needed to gain a better understanding of the underlying social dynamics and learning processes that are involved.

The problems associated with the *digital divide* are likely to persist even when people have obtained access to cyberspace. Evidence from the Oxford Internet Survey in 2003 suggests that there is lower trust of the Internet among categories of users such as the less affluent or the disabled. For these groups, experience in using the Internet has a particularly disproportionate positive impact, increasing their trust in the Internet and lessening their preconceived concerns about risks. Education and exposure to the Internet may offer a general strategy for coping with the risks and threats to the perceived trustworthiness of this technology. However, education and exposure to the Internet are skewed towards higher socio-economic groups. As a result, these strategies could actually reinforce the 'digital divide' in access to the Internet. Other survey data (MORI 2003) suggest that there is considerable public ignorance about what happens to personal data when it is used by public agencies. Overall, there is gap in the evidence base in this area partly because of the lack of comparable and systematic data.

1.22 Cyberspace Market Evolution, the Policy Context, and Privacy

We examined the economic dynamics of the evolution of cyberspace technology and service markets and the interaction of these features with policy measures and the legislative environment in section 6.0. A key observation about market dynamics and the changing legislative policy context is that the development of cyberspace is a global phenomenon. In the future, monitoring global developments will continue to be very important. Effective monitoring across a wide range of issues is essential for effective national crime prevention strategies.

The special characteristics of these markets are an important consideration in understanding how cyberspace technologies will evolve and whether there will be incentives to invest in more dependable and secure systems. Industrial structure, conduct and performance analysis can be used to address this issue. The analysis in section 6.1 ('The Economics of Emerging Cyberspace Markets') shows how asymmetrical information between firms and their customers can lead to customer 'lock-in', often leading to the emergence of dominant firms. Firms will use trust in a variety of ways, sometimes to achieve a form of lock-in to the market, which is in a 'low trust equilibrium' in which there are few incentives to invest in more dependable systems.

262 See section 5.3.

In cases where there are few suppliers competing in the market, a small number of supplier firms can influence the rate of investment in new technologies through their influence over supply and price. In addition, analysis suggests that when firms compete in electronic marketplaces they encounter new opportunities for using anonymity in ways that make their participation in potentially collusive agreements difficult to detect. At the same time, new technologies can be used by firms to monitor customer behaviour and allegiance to firms because of the customer-related information that is available as a result of new information management systems.

From the customer's perspective, the analysis of cyberspace markets highlights the way new technologies may increase competition by augmenting consumer search capabilities through the use of search engines as intermediaries. However, intermediaries may not act solely in the consumer's interest, given the economic incentives that drive their operations. In addition, in areas such as financial intermediation and electronic payment systems, greater trust may enable such intermediaries to encourage increasing market concentration. Cyber trust agents are essential if effective competition in electronic markets is to be fostered, but it remains uncertain whether the market for certification services will grow rapidly in the future.

The demand for security solutions will be influenced strongly by the costs involved in switching between cyberspace security products on the market. Economic analysis suggests that the sustainability of trust relationships in cyberspace markets may actually depend on *asymmetry* among the participants. 'Improvements' or measures designed to enhance the security of cyberspace products leading to greater symmetry in the marketplace, may actually undermine trust. This indicates again that it is the distribution of trust rather than its level that is central to future economic outcomes and whether they foster technologies that reduce or exacerbate cyberspace vulnerabilities.

The parameters of the European Union's existing legislative framework, which affects decisions about cyber trust and crime prevention, are complex and involve numerous interdependencies.[263] This issue was considered in section 6.2 ('The Legislative and Policy Context for Cyberspace'). Given that perceptions about privacy are closely related to the acceptance of measures to enhance the security of cyberspace, we examined whether the prevailing 'privacy paradigm' is consistent with the need to assess the requirements for improved crime prevention strategies (section 6.2.1).

Privacy protection, in particular, relies on many international instruments, national legislation, self-regulatory or voluntary tools, and privacy enhancing technologies or PETs. Research in this area suggests that PETs cannot provide a 'magic bullet' for solving privacy problems or address issues of identity authentication. It is much more likely that a mix instruments will have to be applied to protect privacy alongside instruments and technologies that are consistent with equity considerations and the collective interests of society.

Given the complexity of cyberspace and varying levels of dependability or trustworthiness, future developments will create new possibilities for opportunistic crime and for privacy intrusions. Although technical solutions for communications and transactions with rigorous authentication may eventually provide a foundation for a higher level of trust in cyberspace, they will also create new threats to privacy. One possibility is to encourage the development of relatively finely grained 'digital principles' that would complement the security and privacy guidelines developed by organisations such as the OECD.[264] Such self-regulatory arrangements might build on developments in autonomous software agent computing, but this will raise issues of privacy protection and surveillance.

263 See RAND Europe 2003a,b.

264 Edwards 2004; OECD 2002.

Surveys in many western countries suggest that people generally have high and increasing levels of concern about privacy.[265] While this may be attributed to various pressure groups or to press coverage of data protection issues, the important point in the context of cyber trust and crime prevention is that discussions about privacy generally presume that *balance* is the main feature of policy responses aimed at protecting individual interests in privacy and other rights and responsibilities.

This view has been criticised by those who believe that insufficient weight is given to collective or community interests. In the future it will be necessary to examine distributional issues and equity concerns within the conventional *privacy paradigm*. This will mean examining who enjoys what privacy and why. This view is another feature of the 'digital divide', suggesting that insofar as there are inequalities in the distribution of privacy protection, the issues need to be treated as a social policy concern.

Very little is known about the distribution of privacy protection in terms of typical socio-economic and demographic categories. Empirical research is needed on this issue. The results would enable privacy protection to be treated as an element of social policy. It could then be debated, together with collective security, in terms of alternatives, such as public or private provision, the costs and benefits, rights and entitlements, and the best way to secure privacy. This is important given that crime prevention will be used to protect citizens from infringements to their privacy, e.g. as a result of theft of their identities. A better understanding of the distributional characteristics of privacy protection would provide an evidence base for considering whether inequalities can be justified and whether public policy and its implementation can alter them.

This raises the issue of how much information about our identities is required for crime prevention purposes and what should constitute informed consent. Research indicates that some people have low levels of trust in those who currently and in the future will manage their personal data in both the public and private sectors. Few web sites today meet existing privacy protection standards and it is unclear whether a focus on limiting encryption will be at the expense of more effective, yet less intrusive, crime prevention interventions. Similar arguments may apply to the use of surveillance, the effectiveness of which has not been empirically demonstrated. The overriding goal should be to reduce crime to 'tolerable' levels without incurring unacceptable privacy intrusions, and to consider the potential benefits of more equitable means of delivering privacy whatever the level of privacy protection that is accepted.

It has been suggested that the development of a Privacy Impact Assessment (PIA) methodology would provide a basis for assessing the actual or potential effects that an activity or policy may have for individual privacy.[266] Further development could help to answer questions such as whether we should see cyberspace and various practices as being safe until proven dangerous, or dangerous until proven safe. A system where the role of the 'precautionary principle' in privacy protection is more explicit could become increasingly important,[267] especially if consideration is given to how and when (and when not) to apply it. Measures will be needed to resolve tensions between individual privacy and collective security and to assess the adequacy and enforceability of data protection and freedom of information legislation. Resolution of ethical issues in the contexts where privacy issues come to the fore will play a key role in determining the acceptability of crime prevention measures.

265 See Bennett and Raab 2003, Ch. 3; Bennett 1992, pp. 37-43

266 Raab 1995, 2003; Stewart, 1996.

267 European Commission 2000; European Union Council 1999; Raab 2004.

1.23 Lessons for the Future

The scientific evidence yields insights into the way technical innovation is intersecting with human capacities for learning about cyberspace developments. In each of the areas we have addressed in this report there are uncertainties about the trade-offs that will accompany future human and technical measures to develop more dependable and secure cyberspace systems that would help to minimise the risk of new 'conjunctures of criminal opportunity'. Some of these trade-offs are summarised in

Table 8.

The literature on risk and trust formation and their relationships to the design and implementation of cyberspace systems emphasises the importance of values, reciprocity, information management and human and technical capabilities.

Table 8 Cyberspace and the Potential Trade-offs

Software Dependability	User Requirements, Cost and Complexity
Identification	Anonymity
Authentication of software, data objects and people	Privacy Protection
Type 1 False Rejection Errors	Type 2 False Acceptance Errors
Cyberspace Security	Cyberspace Usability
Risk	Trust and Trustworthiness
Libertarian, Open Networks	Network Control, Surveillance
Informed Debate	'Moral Panic'
Individual Privacy	Collective Interest
Liability	Risk and Cost
Security	Economic Growth and Innovation

Available research is inconclusive with respect to the implications of interventions in cyberspace by those who seek to minimise crime. Given the relatively weak scientific evidence in key areas, there is a need to consider the ethical positions associated with crime prevention measures and to draw inferences about their impact. In some of the areas addressed in this report, the lack of systematic and comparable quantitative evidence means the foundation for evidence-based decision-making will be weak. In these areas, it will be important to consider the ethical positions and to reach judgements. Critical reasoning can be applied to reach such assessments – subject to review as new evidence accumulates - about 'acceptable' and 'unacceptable' levels of trustworthiness of the cyberspace system. This is essential for evaluations of the distributional issues associated with intrusive privacy protection measures and of the benefits of crime protection.

It is clear that:

- Improved crime prevention in cyberspace depends upon a better understanding human motivations and practices and the way these are embedded within complex cyberspace systems;

- Problems facing crime preventers will not be solved by better technology alone; enforcement of behavioural change consistent with 'good' behaviour in cyberspace will mean enabling people to do the 'right' thing easily with substantial implications for the usability and cost of cyberspace technologies;

- Trust in cyberspace can be fostered in both technical and non-technical ways; the options that should be fostered need to be considered in the light of studies of risk perception and the actual risk encountered in cyberspace and in the wider situation;

- Crime prevention measures for cyberspace will need to receive widespread consent nationally and internationally if they are to be effective;

- The dependability of future cyberspace systems and the extent to which they ensure human safety and well-being are matters of human choice; understanding the human and non-human relationships often requires an assumption that it is feasible to believe that agents, both human and technological, will act, or in the case of the latter, will have been designed and implemented to act, in rational or at last quasi-rational ways.

The scale of the challenge facing government policy makers is vast. The speed at which the machinery of government operates can be slow relative to the potential rate of technological change and further slowing of the decision making process due to the need to adopt international solutions may become a larger problem. There are also concerns about introducing legislative and governance solutions, which may manage risks more effectively, but stifle innovation and competitiveness. When new measures are introduced, they interact with other measures often giving rise to unexpected outcomes that may be inconsistent with policy – or indeed, with changing social mores.

No 'future-proof' set of measures can be put in place through unilateral action because the positions of stakeholders are changing and insufficiently clear. Partnerships will be needed between the public and private sectors, working with civil society representatives, to create an accepted framework for cyber trust and crime prevention. Lessons must be learned from policy and regulatory initiatives and f the corresponding failures and successes of these initiatives. There are several *research frameworks* (new frameworks for dependable software engineering, the criminal opportunity models, the social amplification of risk framework, and the privacy impact assessment framework) that could be further developed and interconnected to increase understanding of security measures and crime prevention strategies. Crime prevention, especially in cyberspace, occurs in a rapidly changing technical, economic and social context where unforeseeable properties emerge. The key knowledge about what works as a crime prevention strategy is a wasting asset that must be constantly replenished if crime preventers are to innovate faster than criminals.

This review and synthesis of the existing scientific evidence in a number of key areas has identified gaps in research that is underway in the UK (these are summarised in Appendix B). All of these would benefit from cross-disciplinary investigation. This work will need to include research on the dependability and trustworthiness of all aspects of the cyberspace system. There is, in particular, a need to promote cyberspace system design: that enables users to manage their privacy and their security and for crimes to be prevented or detected; and that encourages greater system reliability and robustness, while maintaining a degree of transparency for users. This must include ensuring appropriate levels of investment in research and development in cyberspace systems, advanced knowledge services, management and engineering and in information assurance initiatives. There is also a need for a collaborative approach across the research community that will harness the considerable breadth of expertise that is available and help to overcome existing fragmentation.

Research needs to be complemented by investment in adequate levels of education and to build awareness of cyberspace developments and crime prevention measures. Many ethical and moral issues are raised by innovations in ICTs, which must be debated in the future. Effort must not become exclusive to only the 'experts', thereby exacerbating 'digital divides'. Building confidence in the information provided by government about the risks to those who encounter cyberspace and

about the trustworthiness of cyberspace systems is essential. The social and economic threats from the social fragmentation and exclusion that will arise if some groups take up the new technologies and benefit from them, but others do not, must also be examined.

The complexity of cyberspace and its emergent properties means that it will be essential to develop methodologies for testing when changes in the human and technical system are likely to create new vulnerabilities. Only in this way will it be feasible to encourage alternative action. The greatest challenge in the future will be managing emergent properties and vulnerabilities in ways that respect changing individual and collective values.

APPENDIX A: LIST OF SCIENCE REVIEWS

Backhouse, J. with Bener, A., Chauvidul, N., Wamala, F., and Willison, R. (2004) 'Social Risk Management – Practices and Behaviour in Cyberspace', report prepared for the Foresight Cyber trust and Crime Prevention Project, London.

Cave, J. (2004) 'The Economics of Trust Between Cyber-Partners', University of Warwick, January.

Dutton, W. H. and Shepherd, A. (2004) 'The Social Dynamics of Cyber Trust: Confidence and Risk on the Internet'. Oxford Internet Institute, University of Oxford, report prepared for the Foresight Cyber Trust and Crime Prevention Project, London.

Jackson, J., Allum, N. and Gaskell, G. (2004) 'Public Perception of Risk: A Review of the Research Literature', London School of Economics and Political Science, report prepared for the Foresight Cyber Trust and Crime Prevention Project, London.

Jones, C. and Randell, B. (2004) 'Dependable Pervasive Systems', University of Newcastle upon Tyne, report prepared for the Foresight Cyber Trust and Crime Prevention Project, London.

O'Hara, K. and Shadbolt, N. (2004) 'Cybertrust, Knowledge Technologies and the Semantic Web', University of Southampton, report prepared for the Foresight Cyber Trust and Crime Prevention Project, London.

Piper, F., Schwiderski-Grosche, S., and Robshaw, M. J. B. (2004) 'Identification and Authentication', Royal Holloway, University of London, report prepared for the Foresight Cyber Trust and Crime Prevention Project, London.

Raab, C. D. (2004) 'New Departures in Privacy Protection', School of Social and Political Studies/Politics, The University of Edinburgh, report prepared for the Foresight Cyber Trust and Crime Prevention Project, London.

Ramchurn, S. D. and Jennings, N. R. (2004) 'Trust in Agent-Based Systems', University of Southampton, report prepared for the Foresight Cyber Trust and Crime Prevention Project, London.

Sasse, M. A. (2004) 'Usability and Trust Issues in Cyberspace', University College London, report prepared for the Foresight Cyber Trust and Crime Prevention Project, London.

APPENDIX B: POTENTIAL FOR CROSS-DISCIPLINARY RESEARCH

Dependable Pervasive Systems

- Achieving adequate operational dependability from large complex software systems when they are deployed is a critical research programme and will remain so for some time – adequate resources are needed to support this work.
- Socio-technical and technical dependability expertise will be required.
- A key question is at what level does system failure become unacceptable and how does the perception of this level differ across user groups?
- Research is needed on the four basic dependability technologies – fault prevention, fault removal, fault tolerance and fault forecasting.
- Research is also needed on the feasibility of developing warrantable software and systems that industry values sufficiently to bear the cost of deployment.
- There is a continuing need for a fundamental review of the problems in software engineering including formal methods and the creative art of software development.
- Research on software project organisation, involvement of end-users/customers in design and implementation and with a concern for the usability of security mechanisms is needed.
- Research is needed on the appropriate balance between evidential - investigative – preventative computer forensics that could be struck and on the risks and benefits of options.

Risk Perception and the Experience of Cyberspace

- In cognitive psychology, e.g. Prospect Theory, should be applied to investigate the heuristics that influence how people experience cyberspace and the likelihood of stereotyping perpetrators (especially in the media), contexts and places influence risk perceptions and whether this has a greater impact than expert reassurance.
- Psychometric research should be applied to determine whether intensive users of ICTs have a sense of familiarity and control that inoculates them against a sense of risk while also leading to a sense of complacency about criminal activity - how attentive are people to threat-related stimuli in cyberspace?
- Research is needed on security and risk to develop the ‘criminal opportunity model’.
- The SARF approach should be applied to cyberspace and crime prevention to provide a means of understanding the communication of risk and how it shapes public perceptions.
- Studies should be made of how learning and risk perception are related to ICT system design and implementation.
- The complexity of individual beliefs, motivations and actions in cyberspace requires longitudinal surveys; international comparative studies such as participation in the World Internet Project by the Oxford Internet Institute, are needed.

Security, Trust and Trustworthiness

- Research is needed on whether trust in cyberspace follows the trustworthiness of systems – how do people place trust and refuse to trust?
- Research is needed on modelling that has a greater capacity to take the contexts of agent interactions into account.
- Research is required on the trustworthiness of the information acquisition processes in the knowledge acquisition process and the consequences for trusting behaviour.
- Research is needed on effective procedures for the maintenance of knowledge bases.

- Continuing research is needed on the viability of various biometrics techniques from market and usability standpoints.
- Research is needed on the means to establish primary secondary verification of 'the original' identity and the development of products that secure the transmission between the biometric sensor and the matching module.
- Research is needed on perceptions of intrusive measures such as the use of DNA samples and chip insertions in the body and on the physical consequences of implanting chips for life.
- Analysis of how security, trust and trustworthiness are signalled in open global network environments, drawing in part on signalling theory from economics as well as on cultural theory, is required.
- Studies of the impact of ICT legacy applications and system features and the potential for lock-in in emerging markets and the mechanisms giving rise to market failures in these markets, especially with regard to trust services, are needed.
- Empirical research is needed on the formation of trust via technical channels and on how best to encourage usable ICT designs.
- Research is needed on the semantics of security to develop a better understanding of the security 'universe of discourse' to facilitate communication and policy development.
- Research methodologies should be developed for investigating organisational risk management using new combinations problem structuring methods and ethnographic methods to provide and evaluate risk management decision support in a variety of organisational settings.
- Research is needed to encourage social values and behavioural changes to inculcate values of society in the use of shared cyberspace with a focus on attitudes towards rights and responsibilities and to establish the factors that favour acceptance of these spaces as safe, secure and reliable.
- Research is needed on PETs and the appropriate allocation of control over cyberspace as between users and system designers and operators.
- Research is needed on the notion of balancing cost and risk, and reward by developing a methodology for investigating the effects of different (portfolio) management strategies.

Risk, Precautionary Measures and Innovation

- Research is needed to establish whether precautionary measures are likely to lead to a failure to take advantage the benefits of new technologies. In particular, there is a need to develop the 'Privacy Impact Assessment' (PIA) methodology.
- Research is required on the distribution of capabilities for privacy protection within different groups of the population.
- Research is needed on the potential trade-offs between productivity gains and the levels of 'acceptable' risk.
- Evaluations are needed of whether crime that is linked to cyberspace developments is being kept within tolerable limits and of whether they perceived riskiness of cyberspace is diminishing over time.

Policies, Principles and Legislation

- Qualitative and experimental research is needed to examine the relevance to cyber trust and crime prevention of past research and the effectiveness of actual policies and techniques that are being applied.
- Research is needed on international developments and distinctive approaches to legislation, policy and regulation.
- Research is required on the epidemiology of cyberspace attacks to identify 'treatment' or policy intervention points taking an analogy with HIV/AIDS insofar as the scale of the problem and development of possible strategies for treating individuals and slowing the spread of infection has only been possible after a thorough understanding of the epidemiology of the disease was achieved.

- Research is needed on the implications of software liability approaches including the development of new ‘Digital Principles’.

Futures Research

- Futures work is needed to consider the potential future impacts of today’s applications, together with those of potential future applications deriving from today’s science base.

APPENDIX C: EUROPEAN UNION AND UNITED KINGDOM RELEVANT LEGISLATION

European Commission (2000) 'EU's Communication on Precautionary Principle', Brussels, 2 February, http://www.gdrc.org/u-gov/precaution-4.html accessed 19 Dec 03.

European Commission (2002) 'The Directive on Privacy and Electronic Communications (2002/58/EC), http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html accessed 20 Dec 03.

European Commission, The Electronic Commerce Directive (00/31/EC) & the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002 No. 2013 UK), http://www.dti.gov.uk/industries/ecommunications/electronic_commerce_directive_0031ec.html accessed 20 Dec 03.

European Commission, The Telecoms Data Protection Directive (97/66/EC) & the Telecommunications (Data Protection and Privacy) Regulations 1999 (SI 1999 No. 2093) http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html#overview accessed 20 Dec 03.

European Union Council (1999) 'Council Resolution of 28 June 1999 on Community Consumer Policy 1999 to 2001' (1999/C 206/01), Official Journal of the European Communities, 21 July.

United Kingdom Government, Computer Misuse Act 1990, http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm accessed 10 Jan 04.

United Kingdom Government, Data Protection Act 1988, http://www.hmso.gov.uk/acts/acts1998/19980029.htm accessed 10 Jan 04 (plus 22 or more statutory codes of conduct under the Act).

United Kingdom Government, Electronic Communications Act 2000 Chapter c.7, http://www.uk-legislation.hmso.gov.uk/acts/acts2000/20000007.htm accessed 20 Dec 03.

United Kingdom Government, The Human Rights Act 1998, http://www.hmso.gov.uk/acts/acts1998/19980042.htm accessed 10 Jan 04.

United Kingdom Government, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, http://www.hmso.gov.uk/si/si2000/20002699.htm accessed 10 Jan 04.

United Kingdom Government, Regulation of Investigatory Powers Act 2000, http://www.hmso.gov.uk/acts/acts2000/20000023.htm accessed 10 Jan 04.

United Kingdom Government, Statutory Instrument 2003 No. 2426, The Privacy and Electronic Communications (EC Directive) Regulations 2003, http://www.hmso.gov.uk/si/si2003/20032426.htm accessed 20 Dec 03.

REFERENCES

Ackerman, B. (1980) *Social Justice in the Liberal State*, New Haven CT: Yale University Press.

Adams, A. and Sasse M. A. (2001) 'Privacy in Multimedia Communications: Protecting Users, Not Just Data', In A. Blandford, J. Vanderdonkt and P. Gray (eds) *People and Computers XV - Interaction without Frontiers, Joint Proceedings of HCI2001 and ICM2001*, Lille, September, Dordrecht: Springer, pp. 49-64.

Allen, A. (1985) *Uneasy Access: Privacy for Women in a Free Society*, Totowa, NJ: Rowman & Littlefield.

Anderson, R. (2003) 'Cryptography and Competition Policy: Issues with "Trusted Computing"', Cambridge University working paper http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tcpa.pdf accessed 10 Jan 04.

Arndt, H. (1949) 'The Cult of Privacy', *Australia Quarterly*, 21: 69-71.

Austin, J., Cliff, D., Ghanea-Hercock, R. and Wright, A. (2003) 'Large-Scale, Small-Scale Systems', Foresight Cognitive Systems Research Review, http://www.foresight.gov.uk/cognitive.html accessed 11 Feb 04.

Axelrod, R. (1984) *The Evolution of Cooperation*. New York: Basic Books.

Bacharach, M. and Gambetta, D. (2001) 'Trust in Signs', In K. Cook (ed) *Trust in Society*, New York: Russell Sage Foundation, pp. 148-184.

Bacharach, M., Guerra, G. and Zizzo, D. (2001) 'Is Trust Self-fulfilling: An Experimental Study', Oxford University Department of Economics Working Paper 76, http://users.ox.ac.uk/~kebl1218/istrussf.pdf accessed 10 Jan 04.

Backhouse, J., Hsu, W. Y., and McDonnell, A. (2003) 'Toward Public Key Infrastructure Interoperability', *Communications of the ACM*, 46(6): 98-100.

Backhouse, J. with Bener, A., Chauvidul, N., Wamala, F. and Willison, R. (2003) 'Social Risk Management – Practices and Behaviour in Cyberspace', report prepared for the Foresight Cyber Trust and Crime Prevention Project, London.

Barber, B. (1983), *The Logic and Limits of Trust*, New Brunswick NJ: Rutgers University Press.

Bargh, J. A. (1984) 'Automatic and Conscious Processing of Social Information', in R. S. Wyer Jr. and T. K. Srull (eds) *Handbook of Social Cognition*, Vol. 3. Hillsdale NJ: Lawrence Erlbaum.

Bastide, S., Moatti, J.-P., Pages, J.-P., and Fagnani, F. (1989) 'Risk Perception and Social Acceptability: the French Case', *Risk Analysis*, 9: 215-225.

Beck, U. (1992) *Risk Society: Towards a New Modernity*. London: Sage.

Belleflamme, P. and Bloch, F. (2001) 'Market Sharing Agreements and Collusive Networks,' University of London Queen Mary College Working Paper 443, http://www.econ.qmul.ac.uk/papers/docs/wp443.pdf accessed 10 Jan 04.

Bener, A. (2000) 'Risk Perception, Trust and Credibility: A Case in Internet Banking', Department of Information Systems, London School of Economics and Political Science.

Ben-Ner, A. and Putterman, L. (2002), 'Trust in the New Economy', HRRI Working Paper 11-02, University of Minnesota, Industrial Relations Center, abstract http://netec.mcc.ac.uk/WoPEc/data/Papers/hrrpapers1102.html accessed 10 Jan 04.

Bennett, C. J. (1992) *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca NY: Cornell University Press.

Bennett, C. J. and Raab, C. D. (2003) *The Governance of Privacy: Policy Instruments in Global Perspective*, Aldershot: Ashgate.

Bernstein, P. L. (1996) *Against the Gods: The Remarkable Story of Risk*. New York: Wiley & Sons.

BIOVISON (2003) Final Report http://www.eubiometricforum.com/index.php?option=com_docman&task=docclick&bid=6 accessed 10 Jan 04.

BloomBecker, B. (1984) 'Introduction to Computer Crime', in J. Finch and E. Dougall (eds) *Computer Security : A Global Challenge*. Amsterdam: Elsevier - North-Holland.

Bolling, P. (1996) *Privacy and the Politics of Intimate Life*, Ithaca NY: Cornell University Press.

Brostoff, S. and Sasse, M. A (2003) '"Ten Strikes and You're Out": Increasing the Number of Login Attempts Can Improve Password Usability', CHI Workshop on Human-Computer Interaction and security systems, Ft Lauderdale, 1-6 April.

Bourdieu, P. and Passeron, J.-C. (1977) *Reproduction in Education, Society and Culture,* translated by Richard Nice. London, Sage.

Bowker, G. and Star, S. (1999) *Sorting Things Out: Classification and its Consequences*, Cambridge, MA: MIT Press.

Bowles, S. and Gintis, H. (2000) 'Optimal Parochialism: The Dynamics of Trust and Exclusion in Networks', Santa Fe Institute Working Paper, 16 February, http://www.santafe.edu/sfi/publications/Working-Papers/00-03-017.pdf accessed 10 Jan 04.

Brantingham, P. and Brantingham, P. (1991) *Environmental Criminology*. Prospect Heights, IL, Waveland Press.

Brooks, F. P. (1995) *The Mythical Man-Month: Essays in Software Engineering, Anniversary Edition*, 2nd Edition, New York: Addison-Wesley Publishing Co.

Bryen, S. (2002) 'A Collective Security Approach to Protecting the Global Critical Infrastructure', ITU Workshop on Creating Trust in Critical Network Infrastructures', Seoul, 20-22 May, http://www.itu.int/osg/spu/ni/security/docs/cni.09.doc accessed 20 Dec 03.

Callon, M. (2003) 'The Increasing Involvement of Concerned Groups in R&D Policies: What Lessons for Public Powers?' in A. Geuna, A. J. Salter, and W. E. Steinmueller (eds) *Science and Innovation: Rethinking the Rationales for Funding and Governance*, Cheltenham: Edward Elgar, pp. 30-68.

Castells, M. (2001) *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford University Press.

Chauvidul, N. (2003) 'Formality and Informality in Internal Control Systems: A comparative study of control in different social and cultural environments in a global bank', Department of Information Systems, London School of Economics and Political Science.

Checkland, P. (1999) *Soft Systems Methodology. A 30-year Retrospective,* Chichester: John Wiley & Sons.

Chokhani, S. and Ford, W. (2003) 'Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework', Internet Draft, http://www.zvon.org/tmRFC/RFC3647/Output/index.html accessed 10 Jan 04.

Clarke, R. (1995) 'Situational Crime Prevention', in M. Tonry and D. Farrington (eds) *Building a Safer Society. Strategic Approaches to Crime Prevention. Crime and Justice: A Review of Research,* Chicago IL: University of Chicago Press.

Clarke, R. (1997) *Situational Crime Prevention: Successful Case Studies*. Albany NY: Harrow and Heston.

Clarke, R. and Cornish, D. (1985) 'Modelling Offender's Decisions: A Framework for Policy and Research', in M. Tonry and N. Morris (eds) *Crime and Justice: An Annual Review of Research,* Chicago IL: University of Chicago Press.

Clarke, R. and Cornish, D. (2000) 'Rational Choice', in R. Paternoster and R. Bachman (eds) *Explaining Crime and Criminals: Essays in Contemporary Criminological Theory,* Los Angeles, CA: Roxbury Publishing Company.

Clegg, S. (1989) *Frameworks of Power,* London: Sage.

Clore, G. L. and Gasper, K. (2000) 'Feeling is Believing: Some Affective Influences on Belief,' in N. H. Frijda, A. S. R. Manstead and S. Bem (eds) *Emotions and Beliefs: How Feelings Influence Thoughts*, Cambridge: Cambridge University Press.

Collins, B. S. (2004) 'Submission to the Royal Academy of Engineering on Complex Software Projects', January.

Cooper, R. and Ross, T. (1985) 'Product Warranties and Double Moral Hazard', *Rand Journal of Economics,* 16: 103-113.

Cornish, D. and Clarke, R. (1986) 'Situational Prevention, Displacement of Crime and Rational Choice Theory', in K. Heal and G. Laycock (eds) *Situational Crime Prevention: From Theory into Practice,* London: HMSO.

Corritore, C. L., Kracher, B. and Wiedenbeck, S. (2003) 'On-line Trust: Concepts, Evolving Themes, A Model', *International Journal of Human Computer Studies*, 58(6): 737-758.

Courtney, R. (1977) 'Security Risk Analysis in Electronic Data Processing', AFIPS Conference Proceedings NCC, New York: AFIPS Press.

Coventry, L., De Angeli, A., and Johnson, G. (2003) 'Honest It's Me – Self-Service Verification', *CHI Workshop on Human-Computer Interaction and Security Systems*, Ft Lauderdale, 1-6 April.

Cremonini, L., Rathmell, A., and Wagner, C. (2003) 'Cyber Trust & Crime Prevention – Foresight Overview', Annotated Briefing prepared for Office of Science & Technology, UK, by RAND Europe, July.

Cvetkovich, G., and Lofstedt, R. (1999) *Social Trust and the Management of Risk,* London: Earthscan.

Damasio A. R. (1994) *Descartes' Error: Emotion, Reason and the Human Brain*, New York: Grosset/Putnam.

d'Aspremont, C. and Gerard-Varet, L. (1979) 'Incentives and Incomplete Information', *Journal of Public Economics*, 11: 25-45.

Department for Constitutional Affairs (DCA) (2003) **'**Response to the Consultation Paper, For Your Information: How Can the Public Sector Provide People with Information on, and Build Confidence in, the Way it Handles their Personal Details?', Department for Constitutional Affairs, London, http://www.dca.gov.uk/consult/datasharing/datashareresp.htm accessed 10 Jan 04.

Dhamija, R. and Perrig, A. (2000) 'Deja Vu: A User Study. Using Images for Authentication', Proceedings of the 9th USENIX Security Symposium, August 2000, Denver, Colorado

Douglas, M. (1966) *Purity and Danger: An Analysis of Concepts of Pollution and Taboo*. London: Routledge and Kegan Paul.

Douglas, M., and Wildavsky, A. (1982) *Risk and Culture: An Essay on the Selection of Technical and Environmental Dangers*. Berkeley CA: University of California Press.

Durkheim, E. (1893/1984) *The Division of Labour in Society*, London: Palgrave Macmillan.

Dutton, W. H. (1999) *Society on the Line: Information Politics in the Digital Age*, Oxford and New York: Oxford University Press.

Dutton, W. H., Gillett, S. E., McKnight, L. W., and Peltu, M. (2003) 'Broadband Internet: The Power to Reconfigure Access'. *OII Forum Discussion Paper No. 1,* Oxford: Oxford Internet Institute, University of Oxford.

Earle, T., and Cvetkovich, G. (1995) *Social Trust: Toward a Cosmopolitan Society,* Westport CT: Praeger.

Edwards, J. (2004) 'Legislative and Regulatory Issues in Cyber Trust and Crime Prevention', Herbert Smith, London, working paper prepared for the Foresight Cyber Trust and Crime Prevention Project.

Egger, F. N. (2001) 'Affective Design of E-Commerce User Interfaces: How to Maximise Perceived Trustworthiness', in M. Helander, H. M. Khalid, and Tham, (eds) *Proceedings of CAHD: Conference on Affective Human Factors Design,* Singapore, June, pp. 317-324.

Eisenstadt, S. and Roniger, L. (1984) *Patrons, Clients and Friends,* Cambridge: Cambridge University Press.

Ekblom, P. (2004a in press) 'How to Police the Future: Scanning for Scientific and Technological Innovations which Generate Potential Threats and Opportunities in Crime, Policing and Crime Reduction', in M. Smith and N. Tiley (eds) *Crime Science: Prevention and Detection*, Cullompton, Devon: Willan.

Ekblom, P. (2004b) 'The Conjunction of Criminal Opportunity', developed between 2001 and 2004, http://www.crimereduction.gov.uk/learningzone/cco.htm accessed 17 Apr. 04.

Ekblom, P. (2003) 'The Conjunction of Criminal Opportunity: A Framework for Crime Reduction', Home Office Crime and Policing Group, Research Development and Statistics Directorate, London, 3 March, http://www.crimereduction.gov.uk/learningzone/cco.htm#1 accessed 7 Feb 04.

Ekblom, P. (2002) 'Future Imperfect: Preparing for the Crimes to Come', *Criminal Justice Matters*, 46(Winter): 38-40.

Ekblom, P. (1999) 'Can We Make Crime Prevention Adaptive by Learning from Other Evolutionary Struggles?' *Studies on Crime Prevention*, 8(1): 27-51.

Ekblom, P. (1997) 'Grearing Up Against Crime: A Dynamic Framework to Help Designers Keep Up with the Adaptive Criminal in a Changing World, *International Journal of Risk, Security and Crime Prevention*, 2(4): 249-65.

Ekblom, P. (1996) 'Towards a Discipline of Crime Prevention: A Systematic Approach to its Nature, Range and Concepts', In T. Bennett (ed) 'Prevention Crime and Disorder: Targeting Strategies and Responsibilities*',* Cambridge: Institute of Criminology.

Electronic Privacy Information Centre (1997) 'Surfer Beware: Personal Privacy and the Internet,' June, http://www.epic.org/reports/surfer-beware.html accessed 10 Jan 04.

Ellison C. (1997) 'What do You Need to Know about the Person with Whom You Are Doing Business?' Written testimony of Carl M. Ellison to the U.S. House of Representatives Science and Technology Subcommittee, Hearing of 28 October 1997: Signatures in a Digital Age, http://world.std.com/~cme/html/congress1.html accessed 13 Nov 2003.

Epstein, S. (1994) 'Integration of the Cognitive and Psychodynamic Unconscious', *American Psychologist*, 49: 709-724.

European Commission (2000) 'EU's Communication on Precautionary Principle', Brussels, 2 February, http://www.gdrc.org/u-gov/precaution-4.html accessed 19 Dec 03.

European Commission (2003) *Third European Report on Science & Technology Indicators 2003 – Towards a Knowledge-based Economy.* Brussels, http://www.cordis.lu/indicators/third_report.htm accessed 20 Dec 03.

European Commission, IST Advisory Group (2002) 'IST Advisory Group – Trust, Dependability, Security and Privacy for IST in FP6', June, http://www.mcst.org.mt/public/01_Sixth%20Framework%20Programme/02_Information%20Society%20Technologies/Reports%20and%20Publications/istag_kk4402464encfull.pdf accessed 20 Dec 03.

European Union Council (1999) 'Council Resolution of 28 June 1999 on Community Consumer Policy 1999 to 2001' (1999/C 206/01), *Official Journal of the European Communities*, 21 July.

Felson, M. (1987) *Crime and Everyday Life*, Thousand Oaks CA: Pine Forge Press.

Felson, M. (1992) 'Routine Activities and Crime Prevention: Armchair Concepts and Practical Action', *Studies on Crime and Crime Prevention,* 1: 31-34.

Fesseden-Raden, J., Fitchen, J. and Heath, J. S. (1987) 'Providing Risk Information in Communities: Factors Influencing What is Heard and Accepted', *Science, Technology and Human Values*, 12(3/4), 94-101.

Finucane, M. L., Alhakami, A. S., Slovic, P. and Johnson, S. M. (2000) 'The Affect Heuristic in Judgments of Risk and Benefits', *Journal of Behavioral Decision Making*, 13, 1-17.

Fitzgerald, J. (1978) 'EDP Risk Analysis for Contingency Planning', *EDP Audit Control and Security Newsletter,* 6(August): 1-8.

Flaherty, D. (1989) *Protecting Privacy in Surveillance Societies: The Federal republic of Germany, Sweden. France, Canada, and the United States*, Chapel Hill NC: University of North Carolina Press.

Fogg, B. J. (2003) *Persuasive Technology. Using Computers to Change What We Think and Do* San Francisco CA: Morgan Kaufmann.

Forester, T. and Morrison, P. (1994) *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. Cambridge MA: MIT Press.

Freeman, C. and Louça, F. (2001) *As Time Goes By: From the Industrial Revolutions to the Information Revolution*, Oxford: Oxford University Press.

Freudenberg, W. R. (1993) 'Risk and Recreancy: Weber, the Division of Labor, and the Rationality of Risk Perceptions', *Social Forces*, 71(4): 909-932.

Friedman, B., Howe, D. C. and Felten, E. (2002) 'Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design', Proceedings of the Thirty-Fifth Annual Hawaii International Conference on System Sciences. Abstract, p. 247, OSPE101. IEEE Computer Society: Los Alamitos, CA, http://www.hicss.hawaii.edu/HICSS_35/HICSSpapers/PDFdocuments/OSPEI01.pdf accessed 10 Jan 04.

Frijda, N. H., Manstead, A. S. R. and Bem, S. (2000) 'The Influence of Emotions on Beliefs', In N. H. Frijda, A. S. R. Manstead and S. Bem (eds) *Emotions and Beliefs: How Feelings Influence Thoughts*, Cambridge: Cambridge University Press.

Frith, U. and Blakemore, S.-J. (2003) 'Social Cognition', Foresight Cognitive Systems Project, Research Review, http://www.foresight.gov.uk/ accessed 20 Dec 03.

Froomkin, A. M. (1996) 'The Essential Role of Trusted Third Parties in Electronic Commerce.' *Oregon Law Review,* 75(Sprint): 49.

Fukuyama, F. (1995) *Trust: The Social Virtues and the Creation of Prosperity*, New York: Free Press.

Gal-Or, E. (1989) 'Warranties as a Signal of Quality', *Canadian Journal of Economics*, 22(1): 50-61.

Gandy, O. (1993) *The Panoptic Sort: A Political Economy of Personal Information*, Boulder CO: Westview Press.

Gibbons, R. (1992) *Game Theory for Applied Economics*, Princeton NJ: Princeton University Press.

Gibson, W. (1984) *Neuromancer*. New York: Ace Books.

Giddens, A. (1991) *Modernity and Self-identity: Self and Society in the Late Modern Age*. Stanford CA: Stanford University Press.

Glaeser, E., Laibson, D. Scheinkman, J. and Soutter, C. L. (2000) 'Measuring Trust', *The Quarterly Journal of Economics*, 115: 811-846.

Goodman, S. E., Hassebroek, P. B., King, D. and Ozment, A. (2002) 'International Coordination to Increase the Security of Critical Network Infrastructures', ITU Workshop on Creating Trust in Critical Network Infrastructures', Seoul, 20-22 May, CNI/04, http://www.itu.int/osg/spu/ni/security/docs/cni.04.doc accessed 20 Dec 03.

Gotoh, R. (2003) 'For Building e-Confidence: A Proposal for the Trusted Third Party Model', *National Institute of Informatics (NII) Journal,* 6, http://www.nii.ac.jp/hrd/HTML/Journal/pdf/06/06-06.pdf accessed 10 Jan 04.

Gray, J. (1995) *Enlightenment's Wake: Politics and Culture at the Close of the Modern Age*, London: Routledge.

Green, J. M. (1995) *Risk, Rationality and Misfortune: Towards a Sociology of Accidents*. London: UCL Press.

Guerra, G., Zizzo, D., Dutton, W. and Peltu, M. (2003) 'Economics of Trust in the Information Economy: Issues of Identity, Privacy and Security' Oxford Internet Institute, University of Oxford Working Paper, April, http://www.oii.ox.ac.uk/resources/publications/OIIRR_ElectronicTrust_0403.pdf accessed 10 Jan 04.

Guerra, G. and D. Zizzo (2002) 'Trust Responsiveness and Beliefs', Oxford University Department of Economics Working Paper 99, http://www.econ.ox.ac.uk/Research/WP/PaperDetails.asp?PaperID=131 accessed 10 Jan 04.

Hardin, R. (1991) 'Trusting Persons, Trusting Institutions', in R. Zeckhauser (ed) *Strategy and Choice*, Cambridge MA: MIT Press, pp. 185-209.

Hawkins, R. W., Mansell, R. and Steinmueller, W. E. (1999) 'Toward Digital Intermediation in the Information Society', *Journal of Economic Issues,* XXXIII(2): 383-391.

Himanen, P. (2001), *The Hacker Ethic*, London: Secker & Wargurg.

Hindelang, M., M. Gottfredson, et al. (1978) *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimisation*. Cambridge, MA: Ballinger.

Hirschi, T. (1969) *Causes of Delinquency*. Berkeley and Los Angeles CA: University of California Press.

Hitchings, J. (1995) 'Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology', *Computers & Security,* 14(5): 377-383.

Hofstede, G. (1991) *Cultures and Organisation – Software of the Mind – Intercultural Cooperation and Its Importance for Survival*, New York: McGraw-Hill.

Hollis, M. (1998). *Trust Within Reason*, Cambridge: Cambridge University Press.

Horlick-Jones, T., Sime, J. and Pidgeon, N. (2003) 'The Social Dynamics of Environmental Risk Perception: Implications for Risk Communication Research and Practice', in N. Pidgeon, R. E. Kasperson and P. Slovic (eds) *The Social Amplification of Risk*. Cambridge: Cambridge University Press, pp. 262-85.

Independent (2003) 'Gone Phishing', *The Independent,* 17 December, http://news.independent.co.uk/digital/features/story.jsp?story=473895 accessed 17 Jan 03.

Institute for Prospective Technological Studies (2003), 'Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview', Institute for Prospective Technological Studies, Saville, July.

Jackson, J. (2003) 'An Analysis of a Debate and Construct', in H. Albrecht, T. Serassis, and H. Kania, (eds) *Images of Crime Volume II,* Freiburg: Edition Iuscrim (Max Planck Institute).

Jackson, M. and Watts, A. (2002), 'On the Formation of Interaction Networks in Social Coordination Games', *Games and Economic Behaviour*, 41: 265-291.

Johansen, R. (1988), *Groupware*, New York: Free Press.

Kahneman, D., and Tversky, A. (1979) 'Prospect Theory: Analysis of Decision under Risk', *Econometrica*, 47(2): 263-291.

Kahneman, D., Slovic, P., and Tversky, A. (Eds) (1982) *Judgment under Uncertainty: Heuristics and Biases,* Cambridge: Cambridge University Press.

Kasperson, J. X., Kasperson, R. E., Pidgeon, N. and Slovic, P. (2003) 'The Social Amplification of Risk: Assessing Fifteen Years of Research and Theory', In N. Pidgeon, R. E. Kasperson and P. Slovic (eds) *The Social Amplification of Risk*. Cambridge: Cambridge University Press, pp. 13-46.

Kasperson, R. E., Renn, O. and Slovic P. (1988) 'Social Amplification of Risk: A Conceptual Framework', *Risk Analysis*, 8: 177-187.

Katz, M. and Shapiro, C. (1994) 'Systems Competition and Networks Effects', *Journal of Economic Perspectives*, 8: 93–115.

Kent, S. T. and Millett, L. I. (eds) (2003) *Who Goes There? Authentication Through the Lens of Privacy,* Washington DC: National Academy Press.

Kleinig, J. (2000) 'The Burdens of Situational Crime Prevention', in A. von Hirsh, D. Garland and A. Wakefield (eds*) Ethical and Social Perspectives on Situational Crime Prevention,* London: Hart.

Knack, S. and Keefer, P. (1997) 'Does Social Capital have an Economic Payoff?', *Quarterly Journal of Economics,* 112(4): 1251-1288.

Krimsky, S. and Plough, O. (1988) *Environmental Hazards: Communicating Risks as a Social Process*, Dover MA: Auburn House.

Latham, R. (ed) *From Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Society*, New York: New Press.

Laudon, K. (1996) 'Markets and Privacy', *Communications of the Association for Computing Machinery*, 39: 92-104.

Lessig, L. (1999) *Code and Other Laws of Cyberspace*, New York: Basic Books.

Levi, M. (2001) '"Between the Risk and the Reality Falls the Shadow" - Evidence and Urban Legends in Computer Fraud', in D. S. Wall (ed) *Crime and the Internet*, London: Routledge, pp. 44-58.

Liberatore, A. (2000) 'From Science/Policy Interface to Science/Policy/Society Dialogue', paper for the conference 'The contribution of social sciences to knowledge and decision making', Bruges, 26-28 June.

Loewenstein, G. F., Weber, E. U., Hsee, C. K. and Welch, E. S. (2001) 'Risk as Feelings', *Psychological Bulletin*, 127, 267-286.

Lohse, G. L., Bellman, S., and Johnston, E. J. (2000) 'Consumer Buying Behavior on the Internet: Findings from Panel Data', *Journal of Interactive Marketing*, 14: 15- 29.

Luhmann, N. (1979). *Trust and Power*. Chichester: John Wiley & Sons.

Lunn, R. J., and Suman, M. W. (2002) 'Experience and Trust in Online Shopping', in B. Wellman and C. Haythornthwaite (eds) *The Internet in Everyday Life,* Oxford: Blackwell Publishers, pp. 549-77.

Lutz, N. (1989) 'Warranties as Signals under Consumer Moral Hazard', *Rand Journal of Economics* 20(2): 239-255.

Lyon, D. (1994) *The Electronic Eye: The Rise of Surveillance Society*, Minneapolis, MN: University of Minnesota Press.

Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*, Milton Keynes: Open University Press.

MacKenzie, D. (1999) 'The Certainty Trough', in W. H. Dutton (ed) *Society on the Line,* Oxford: Oxford University Press, pp. 43-6.

Mahbubani, K. (2002) *Can Asians Think? Understanding the Divide Between East and West*, South Royalton, VT: Steerforth Press.

Manasian, D. (2003) 'Caught in the Net', *The Economist*, 23 January.

Mansell, R., Schenk. I. and Steinmueller, W. E. (2000) 'Net Compatible: The Economic and Social Dynamics of E-commerce', *Communications & Strategies,* 38(2): 241-276.

Mansell, R. and Steinmueller, W. E. (2000) *Mobilizing the Information Society: Strategies for Growth and Opportunity,* Oxford, Oxford University Press.

Marx, G. (1988) *Undercover: Police Surveillance in America*, Berkeley, CA: University of California Press.

Marx, G. (1999) 'Ethics for the New Surveillance', in C. Bennett and R. Grant (eds) *Visions of Privacy: Policy Choices for the Digital Age*, Toronto: University of Toronto Press, pp. 38-67.

Matsumoto, T. (2002) 'Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies – A Case Study for User Identification', Yokohama National University, presentation to ITU-T Workshop on Security, Seoul, 14 May http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf accessed 17 Jan 04.

Macaulay, S. (1963) 'Non-Contractual Relations in Business', *American Sociological Review,* 28: 55-70.

McClue, A. (2003) 'Nationwide Ditches Iris and Fingerprint Biometrics', 23 September http://www.silicon.com/software/security/0,39024655,10006129,00.htm accessed 10 Jan 04.

McKnight, D. H. and Chervany, N. L. (2000) 'What is Trust? A Conceptual Analysis and An Interdisciplinary Model', In Proceedings of the American Conference on Information Systems 2000, pp. 827-833.

Mill, J. S. (1869) *On Liberty*. London: Longman, Roberts and Green (republished New York: Bartleby, Com 1999 http://www.bartleby.com/130/ accessed 7 Feb 2004.

Miller, P. (2003) 'The See-through Society: Openness and the Future of the Internet', DEMOS, London, Note prepared for the Foresight Cyber Trust and Crime Prevention Project, London.

Mitchell, W. J. (1996) *City of Bits: Space, Place and the Infobahn*. Cambridge MA: The MIT Press.

Moreh, J. (1997) 'Digital Certificates and Certificate Authorities', Database Web Advisor, September.

Morris, S. (2000) 'Contagion', *Review of Economic Studies*, 67: 57-78.

MORI (2003) *Privacy and Data-Sharing: Survey of Public Awareness and Perceptions*, Research Study Conducted for Department for Constitutional Affairs, MORI, London.

Morris, R., Hitch, G., Graham, K., and Bussey, T. (2003) 'Learning and Memory', Foresight Cognitive Systems Project, Research Review, http://www.foresight.gov.uk/ accessed 20 Dec 03.

Murdock, G., Petts, J. and Horlick-Jones, T. (2003) 'After Amplification: Rethinking the Role of the Media in Risk Communication', in N. Pidgeon, R. E. Kasperson and P. Slovic (eds) *The Social Amplification of Risk*. Cambridge: Cambridge University Press, pp. 156-78.

National Hi-Tech Crime Unit (2004) 'Hi-Tech Crime: The Impact on UK Business, report by the National Hi-Tech Crime Unit', London at: http://www.nhtcu.org/ accessed 16 Apr 2004.

Naughton, J. (1999) *A Brief History of the Future*, London: Phoenix.

OECD (2000) 'Building Trust in the Online Environment: Business to Consumer Dispute Resolution', Orientation Documents at the Joint Conference of the OECD, HCOPIL, ICC, Hague, Netherlands, December 11-12, p.5.

OECD (2002) 'Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security', Paris: OECD.

O'Hara, K. (2004a) 'The Ethics of Cyberstruct', Note prepared for the Foresight project on Cyber Trust and Crime Prevention, Intelligence, Agents, Multimedia Group, Department of Electronics and Computer Science, University of Southampton, 3 January.

O'Hara, K. (2004b) *Trust: From Socrates to Spin*, Cambridge: Icon Books.

O'Hara, K., Hall, W., van Rijsbergen, K. and Shadbolt, N. (2003) 'Memory, Reasoning and Learning', Foresight Cognitive Systems Project, Research Review, http://www.foresight.gov.uk/ accessed 20 Dec 03.

O'Neill, O. (2000) *Bounds of Justice.* Cambridge: Cambridge University Press.

O'Neill, O. (2002) *Autonomy and Trust in Bioethics.* Cambridge: Cambridge University Press.

O'Siochru, S. and Constanza-Chock, S. (2003) 'Global Governance of Information and Communication Technologies: Implications for Transnational Civil Society Networking', prepared for the Social Science Research Council, New York, http://www.ssrc.org/programs/itic/governance_report/index.page accessed 9 Jan 04.

ONS (Office of National Statistics) (2001) 'First E-commerce Survey of Business', London, 15 May.

Osborne, K. (1998) 'Auditing the IT Security Function', *Computers & Security,* 17(1): 34-41.

Palmer, G (2000) 'The New Spectacle of Crime,' in D. Thomas and B. D. Loader (eds) *Cybercrime Law Enforcement, Security And Surveillance In The Information Age*, London: Routledge, pp. 85-102.

Parker, D. (1997) 'The Strategic Values of Information Security in Business', *Computers & Security* 16(7): 572-582.

Pateman, C. (1983) 'Feminist Critiques of the Public/Private Dichotomy', in S. Benn and G. Gaus (eds) *Public and Private in Social Life*, New York: St. Martin's Press, pp. 281-303.

Perez, C. (2002), *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages*, Cheltenham: Edward Elgar.

Petrie, H. (2002) 'Password Clues', Centralnic, 12 September, http://www.centralnic.com/page.php?cid=77, accessed 10 Jan 04.

Petts, J. Horlick-Jones, T. and Murdock, G. (2001) 'Social Amplification of Risk: The Media and the Public, *Health and Safety Executive Contract Research Report 329/2001.* Sudbury: HSE Books.

Pidgeon, N., Kasperson, R. E. and Slovic, P. (eds) (2003) *The Social Amplification of Risk*. Cambridge: Cambridge University Press.

PIU (Performance and Innovation Unit) (2002) 'Privacy and Data Sharing', London: Performance and Innovation Unit, Cabinet Office.

Pollitt, M. (2001) 'The Economics of Trust, Norms and Networks', Judge Institute of Management Working Paper, Cambridge University, http://www.econ.cam.ac.uk/electricity/people/pollitt/economicstrust.pdf accessed 10 Jan 04.

Poortinga, W., and Pidgeon, N. (2003) 'Public Perceptions of Risk, Science and Governance: Main findings of a British survey of five risk cases', Norwich: Centre for Environmental Risk, University of East Anglia.

Posner, R. (1978) 'An Economic Theory of Privacy', *Regulation*, May/June, pp. 19-26

Putnam, R. D. (2000) *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster.

Putnam, R. D. (1993) *Making Democracy Work: Civic Traditions in Modern Italy*, Princeton NJ: Princeton University Press.

Raab, C. D. (1998) 'Electronic Confidence: Trust, Information and Public Administration', in I. Snellen and van de Donk, W. (eds) *Public Administration in an Information Age: A Handbook,* Amsterdam: IOS Press, pp. 113-33.

Raab, C. D. (1995) 'Connecting Orwell to Athens? Information Superhighways and the Privacy Debate', In W. van de Donk, I. Snellen and P. Tops (eds) *Orwell in Athens: A Perspective on Informatization and Democracy*, Amsterdam: IOS Press, pp. 195-211.

Raab, C. D. (1997) 'Privacy, Democracy, Information', in B. Loader (ed) *The Governance of Cyberspace*, London: Routledge, pp. 155-74.

Raab, C. D. (1999) 'From Balancing to Steering: New Directions for Data Protection', in C. Bennett and R. Grant (eds) *Visions of Privacy: Policy Choices for the Digital Age*, Toronto: University of Toronto Press, pp. 68-93.

RAND Europe (2003a) 'Handbook of Legislative Procedures of Computer and Network Misue in EU Countries for Assisting Computer Security Incident Response Teams (CSIRTs), http://www.iaac.org.uk/csirt/csirtWS-flyer.pdf accessed 22 Feb 04.

RAND Europe (2003b) 'Benchmarking Security and Trust in Europe and the US', Statistical Indicators Benchmarking the Information Society (SIBIS), Report by L. Cremonini and L. Valeri, IST-2000-26276, EC IST Programme, Santa Monica CA http://www.rand.org/publications/MR/MR1736/MR1736.pdf accessed 22 Feb 04.

Ravetz, J. R. (1987) 'Usable Knowledge, Usable Ignorance', *Knowledge: Creation, Diffusion, Utilization*, 9(1): 87-116.

Rawls, J. (1972). *A Theory of Justice*, Oxford: Oxford University Press.

Rayner, S. (1992) 'Cultural Theory and Risk Analysis', in S. Krimsky and D. Golding (eds) *Social theories of risk,* Westport CT: Praeger, pp. 83-114.

Reason, J. (1990) *Human Error*. Cambridge: Cambridge University Press.

Regan, P. (1995) *Legislating Privacy: Technology, Social Values and Public Policy*, Chapel Hill NC: University of North Carolina Press.

Regan, P. (2002) 'Privacy as a Common Good in the Digital World', *Information, Communication & Society*, 5(3): 382-405.

Rice, R. (1984), 'Mediated Group Communication' In Rice, R. and Associates (ed) *The New Media: Communication, Research, and Technology,* Beverly Hills, CA: Sage Publications, pp. 129-54.

Riegelsberger, J., Sasse, M. A. and McCarthy, J. (2003) 'The Researcher's Dilemma: Evaluating Trust in Computer-Mediated Communication', *International Journal of Human Computer Studies*, 58(6): 759-781.

Riegelsperger, J. and Sasse, M. A. (2001) 'Trustbuilders and Trustbusters: The Role of Trust Cues in Interfaces to E-commerce Applications', in B. Schmid, K. Stanoevska-Slabeva, and V. Tschammer (Eds) *Towards the E-Society*. *Proceedings of I3E 2001*, Zurich, Switzerland, October, Amsterdam: Kluwer, Norwell, pp. 17-30.

Rogerson, M. and Pease, K. (2003) 'Privacy, Identity and Crime Prevention', University of Huddersfield, Note prepared for the Foresight Cyber Trust and Crime Prevention Project, London.

Rohrmann, B. (1999) 'Risk Perception Research: Review and Documentation (48)', Julich: Julich Research Centre.

Rosa, E. (2003) 'The Logical Structure of the Social Amplification of Risk Framework (SARF): Metatheoretical Foundations and Policy Implications', In N. Pidgeon, R. E. Kasperson and P. Slovic (eds) *The Social Amplification of Risk*. Cambridge: Cambridge University Press, pp. 47-79.

Royal Academy of Engineering and British Computer Society (2004) 'The Challenges of Complex IT Projects', Report of a working group from The Royal Academy of Engineering and The British Computer Society, London.

Royal Society (2003) 'Potential Wealth-creating Developments from Research in Security: The Next Decade', Royal Society Science, City, Industry Dialogue, Information and Communication Technologies to Enhance the Quality of Life, Report on a seminar held 2 June, London.

Royal Society for the Prevention of Accidents (1992) *Risk: Analysis, Perception and Management*. London: Royal Society.

Rule, J. and Hunter, L. (1999) 'Towards Property Rights in Personal Data', in C. Bennett and R. Grant (eds.), *Visions of Privacy: Policy Choices for the Digital Age*, Toronto: University of Toronto Press, pp. 168-81.

Rule, J., McAdam, D., Stearns, L. and Uglow, D. (1980) *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*, Amsterdam: Elsevier.

Sasse, M. A., Brostoff, S. and Weirich, D. (2001) 'Transforming the 'Weakest Link': A Human-computer Interaction Approach to Usable and Effective Security', *BT Technology Journal*, 19(3): 122-131.

Schacter, D. L. (2002) *The Seven Sins of Memory*. Boston: Mariner Books.

Schneier, B. (2003) *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, New York: Copernicus Books.

Schneier, B. 2000, *Secrets and Lies*, Chichester: John Wiley & Sons.

Schoeman, F. (1992) *Privacy and Social Freedom*, Cambridge: Cambridge University Press.

Sharpe, B. (2003) 'Foresight Cognitive Systems Project – Applications and Impact', DTI Foresight Report for the Cognitive Systems Project, The Appliance Studio Ltd, September, http://www.foresight.gov.uk/cognitive.html accessed 7 Feb 04.

Sharpe, B. and Zaba, S. (2004) 'CTCP Technology: Forward Look', The Appliance Studio Ltd, report prepared for the Foresight Cyber Trust and Crime Prevention Project, London.

Shavell, S. (1987) *Economic Analysis of Accident Law*, Cambridge MA: Harvard University Press.

Short, J., Williams, E., and Christie, B. (1976), *The Social Psychology of Telecommunications,* London: John Wiley & Sons.

Siegrist, M., Cvetkovich, G., and Roth, C. (2000) 'Salient Value Similarity, Social Trust, and Risk/Benefit Perception', *Risk Analysis*, 20(3): 353-362.

Silverstone, R. (2003) 'Media and Technology in the Everyday Life of European Societies', Final Deliverable, The European Media and Technology in Everyday Life Network, 2000-2003, available http://www.lse.ac.uk/collections/EMTEL/main1.html accessed 10 Jan 04.

Sjoberg, L. (1996) 'A Discussion of the Limitations of the Psychometric and Cultural Theory Approaches to Risk Perception', *Radiation Protection Dosimetry*, 68(3-4): 219-225.

Skibell, R. (2002) 'The Myth of the Computer Hacker', *Information, Communication & Society,* 5(3): 336-356.

Slovic, P. (1993) 'Perceived Risk, Trust, and Democracy', *Risk Analysis*, 13(6): 675-682.

Slovic, P., Finucane, M. L., Peters, E., and MacGregor, D. G. (in press) 'Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality', *Risk Analysis*.

Slovic, P., Finucane, M., Peters, E. and MacGregor, D. G. (2002) 'The Affect Heuristic', in T. Gilovich, D. Griffin and D. Kahneman (eds) *Heuristics and Biases: The Psychology of Intuitive Judgment*. New York: Cambridge University Press, pp. 397-420.

Slovic, P., Lichtenstein, S., and Fischoff, B. (1979) 'Which Risks are Acceptable?' *Environment*, 21(4): 17-20.

Slovic, P., Lichtenstein, S., and Fischoff, B. (1980) 'Facts and Fears: Understanding Perceived Risk', in R. C. Schwing and W. A. Albers (Eds) *Societal Risk Assessment: How Safe is Safe Enough?* New York: Plenum, pp. 67-93.

Smith, B. and T. Keehan (1997) 'Digital Signatures: The State of the Art and the Law', *Banking Law Journal* 114**:** 506.

Sobel, J. (2002) 'Can We Trust Social Capital?', *Journal of Economic Literature,* 40(2): 139-54.

Starr, C. (1969) 'Social benefit versus technological risk', *Science*, 165: 1232-1238.

Steinmueller, W. E. (2004) 'Economics and Trust in Cyberspace', Note prepared for the OST Foresight Project on Cyber Trust and Crime Prevention, Southampton University, 2 January.

Stewart, B. (1996) 'Privacy Impact Assessments', *Privacy Law & Policy Reporter*, 3-4: http://www.austlii.edu.au/au/journals/PLPR/1996/39.html accessed 10 Jan 04.

Surman, M. and Reilly, K. (2003) 'Appropriating the Internet for Social Change: Towards the Strategic Use of Networked Technologies by Transnational Civil Society Organizations', prepared for the Social Science Research Council, New York, http://www.ssrc.org/programs/itic/civ_soc_report/index.page accessed 10 Jan 04.

Theil, C. (2001) Voraussetzungen für den Ersatz der PIN bei Geldausgabeautomaten: Bankfachliche Anforderungen. Presentation at BIOTRUST Workshop, 5 June, University of Giessen-Friedberg. Slides available from http://biotrust.de/ws050601/SIZ.pdf accessed 10 Jan 04.

Thomas, D. and Loader, B. D. (eds) (2000) *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. London: Routledge.

Thompson, P. (1999) 'The Ethics of Truth-telling and the Problem of Risk', *Science and Engineering Ethics*, 5(4): 489-510.

Thompson, P., and Dean, W. (1996) 'Competing Conceptions of Risk', *Risk: Health, Safety and Environment,* 7, http://www.piercelaw.edu/risk/vol7/fall/thompson.htm accessed 10 Jan 04..

Torinafacile (2003) http://www.torinofacile.it/ accessed 10 Jan 04.

Tyrrell, P. (2004) 'Realities of a Virtual Economy' *FT.com,* 1 January.

Uslaner, E. M. 2002, *The Moral Foundations of Trust,* Cambridge: Cambridge University Press.

Valentine, T. (1999a) 'An Evaluation of the Passfaces Personal Authentication System', Technical Report, Department of Psychology Goldsmiths College, University of London.

Valentine, T. (1999b) 'Memory for Passfaces After a Long Delay', Technical Report, Department of Psychology Goldsmiths College, University of London.

Varian, H. (2002) 'System Reliability and Free Riding', Economics and Information Security Workshop, Berkeley, CA, http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/49.pdf accessed 10 Jan 04.

Warren, S. and Brandeis, L. (1890), 'The Right to Privacy', *Harvard Law Review*, 4: 193-220.

von Hirsch (2000) 'The Ethics of Public Television Surveillance,' in A. von Hirsh, D. Garland and A. Wakefield (eds*) Ethical and Social Perspectives on Situational Crime Prevention,* London: Hart, pp. 59-67.

von Neuman, J. and Morgenstern, O. (1944) *Theory of Games and Economic Behavior,* Princeton NJ: Princeton University Press.

von Solms, B. (2001). 'Corporate Governance and Information Security', *Computers & Security,* 20(3): 215-218.

Wall, D. S. (ed) (2001) *Crime and the Internet*. London: Routledge.

Wallace, P. (2001), *The Psychology of the Internet,* Cambridge: Cambridge University Press.

Wamala, F. (2002) 'Comparing Public Key Infrastructure Institutionalisation in Two Global Organisations', The *Fuducia* Project, Department of Information Systems, London School of Economics.

Weirich, D. and Sasse, M. A. (2001) 'Pretty Good Persuasion: A first step towards effective password security for the Real World', Proceedings of the New Security Paradigms Workshop, 10-13 September, Cloudcroft, NM, New York: ACM Press, pp. 137-143.

Welsh, B. C. and Farrington, D. P. (2002) 'Crime Prevention Effects of Closed Circuit Television: A Systematic Review', Home Office Research Study 252, London.

Westin, A. (1967) *Privacy and Freedom*, New York: Athenaeum.

Whitten, A and Tygar, D. (1999) 'Why Johnny can't Encrypt: A Usability Evaluation of PGP 5.0',, Proceedings of the 8th USENIX Security Symposium*,* August, Washington DC.

Wiedemann, P. M., Clauberg, M. and Schutz, H. (2003) 'Understanding Amplification of Complex Risk Issues: The Risk Story Model Applied to the EMF Case', in N. Pidgeon, R. E. Kasperson and P. Slovic (eds) *The Social Amplification of Risk*. Cambridge: Cambridge University Press, pp. 286-301.

Williamson, O. E. (2000) 'The New Institutional Economics: Taking Stock, Looking Ahead', *Journal of Economic Literature*, 38(3) 595-613.

Williamson, O. E. (1975) *Markets and Hierarchies: Analysis and Antitrust Implications,* New York: Free Press.

Willison, R. (2002) 'Opportunities for Computer Abuse: Assessing a Crime Specific Approach in the Case of Barings Bank', Department of Information Systems, London School of Economics and Political Science.

Wood, C. (1995) 'Writing InfoSec Policies', *Computers & Security,* 14(8): 667-674.

Woodward Jr., J. D., Orians, N. M. and Higgins, P. T. (2002) *Biometrics*, New York: McGraw-Hill Osborne Media.

Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2002) 'The Memorability and Security of Passwords – Some Empirical Results', Technical Report No. 500, Computer Laboratory, University of Cambridge, http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf accessed 24 January 04.

Yan, J. J. (2001) 'A Note on Proactive Password Checking', Proceedings of the New Security Paradigms Workshop, New York: ACM Press.

Zajonc, R. B. (1980) 'Feeling and Thinking. Preferences Need No Inferences', *American Psychologist*, 35: 151-175.

Zurko, M. E. and Simon, D. (1996) 'User-Centered Security', Proceedings of the New Security Paradigms Workshop, New York: ACM Press.

6, Perri. (1998) *The Future of Privacy, Volume 1: Private Life and Public Policy*, London: Demos.