CORE
Metadata, citation and similar papers at core.ac.uk
Provided by LSE Research Online

Robin Mansell and Brian S. Collins

Introduction: Trust and crime in information societies

Book section

Original citation:
Mansell, Robin and Collins, Brian S. (2005) Introduction: Trust and crime in information societies. In: Mansell, Robin and Collins, Brian S., (eds.) Trust and crime in information societies. Edward Elgar, Cheltenham, UK, pp. 1-10. ISBN 9781847203397

© 2005 Edward Elgar Publishing

This version available at: http://eprints.lse.ac.uk/9000/
Available in LSE Research Online: September 2013

LSE has developed LSE Research Online so that users may access research output of the School. Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Users may download and/or print one copy of any article(s) in LSE Research Online to facilitate their private study or for non-commercial research. You may not engage in further distribution of the material or use it for any profit-making activities or any commercial gain. You may freely distribute the URL (http://eprints.lse.ac.uk) of the LSE Research Online website.

This document is the author's submitted version of the book section. There may be differences between this version and the published version. You are advised to consult the publisher's version if you wish to cite from it.

http://eprints.lse.ac.uk

Chapter 1 Introduction

Robin Mansell and Brian S. Collins

1.1 INFORMATION SOCIETY FUTURES

The future of today's information societies is contingent upon the evolution of cyberspace as 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 cyberspace 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. In some areas, however, there is considerable stability and sufficient understanding of relationships within the system to justify action aimed at improving crime prevention.

The Internet, its future and the experiences of those using it, have become subjects of inquiry for nearly every academic discipline. As the reach of the Internet has become global, it also has become the focus of a growing amount of 'research in the wild' and the subject of argument over the values that should govern its development currently and in the future.[1] Our central concerns in this volume are with the relationships between cyber trust and crime prevention and with some of the key interrelationships between the human and technical components of cyberspace.[2] These concerns coexist with other concerns about what actions might be taken that would interact with those relating to cyber trust and crime prevention.

The chapters in this book are based on papers commissioned by the UK government's Foresight project on Cyber Trust and Crime Prevention.[3] This project, which was formally completed in mid-2004, aimed to explore the application and implications of new generations of information and communications technologies (ICTs) in selected areas that will present opportunities and challenges for crime prevention in the future. In the course of this project consideration was given to the possible drivers, opportunities, threats and barriers to the evolution of cyberspace and to the feasibility of various crime prevention measures. Such measures, in part, will govern

interactions between people and their machines and within a globally networked ‘machine’.

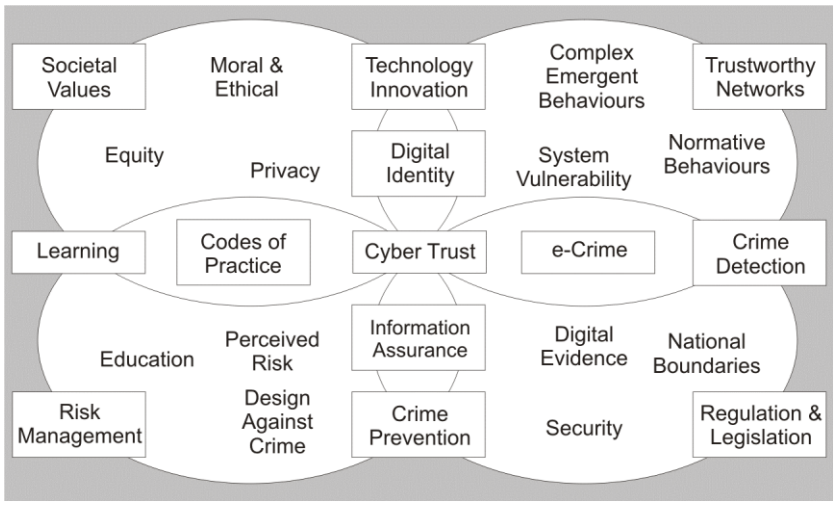
The continuing development of cyberspace raises issues that are fundamental to individual and collective human safety and security. One of the challenges during the project was to distil lessons from the scientific evidence base and to highlight areas in which there are gaps that could be filled by research. The authors of the papers collected in this volume draw upon research within the sciences, the social sciences and the field of engineering. Each of the chapters highlights current understanding of issues that will affect the evolution of cyberspace and the future effectiveness of crime prevention measures. In this introductory chapter, we explain why certain technologies were selected for investigation in the project and give reasons for our focus on such issues as risk, trust and trustworthiness, privacy, security and ethics alongside technology.

As in other areas of technological innovation it is important to assess whether cyberspace developments will give rise to new criminal opportunities. One means of making such an assessment is to examine some of the key features of cyberspace to determine the extent to which people will have greater predispositions to commit crime and to which they will have new resources available to enable them to do so. It is also necessary to examine the extent of the incentives for developers of the cyberspace system to adopt measures that will make cyberspace less attractive for criminals and those who promote crime, for example, by preventing the provision of ‘inside’ information, passwords and tools, and encouraging users not to be careless with their own security.

In a Foresight project of this kind, it is essential to restrict the scope of the inquiry in order to move beyond speculative claims about the likely consequences of cyberspace developments for crime prevention strategies. The principal technologies considered during the project are those that play a major role in managing human and software agent identities and authenticity in cyberspace, in delivering cyber system robustness and dependability, in augmenting the security of cyberspace and in contributing to information assurance and knowledge management.

The topics for state-of-the-art reviews of the existing scientific literature were chosen by an expert panel. This volume provides an entry point to theoretical and empirical work in the topic areas shown in Figure 1.1. 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 1.1 Cyber trust and crime prevention - web of components



At any given time, there will be dominant organizing themes in the spread of cyberspace networks. In 2004, even as the open source software movement was gaining ground, cyberspace technologies were organized largely around corporate and home desktop computing and the 'Wintel' 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 the pace of innovation throughout the ICT industry and for the competitiveness of 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 measures to promote open access to information and new models fostering open source software developments, i.e. 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.

The current and future trends in the development of cyberspace technologies were examined in the Cyber Trust and Crime Prevention project in a variety of contexts and with respect to the many socio-technical and ethical issues that they raise. Analysis of the potential threats to human safety and security in a pervasive cyberspace environment is complicated by

uncertainty about how people will perceive its associated 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. However, public perceptions of cyberspace risk have received relatively little attention, 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.

It is important to acknowledge, nevertheless, that concepts of risk and trust are important for understanding the future development of the cyberspace system. 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 control. It is giving rise to new perceptions of risk and to new meanings and interpretations of developments in cyberspace. People will assess the risks as being more or less serious depending upon how they weigh 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, responsibilities and accountabilities. 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. For instance, problems and perceived dangers may be seen as a failure either of the technical system or of the system designers and users to take steps to prevent crime or to reduce the vulnerabilities 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. Issues of risk and trust, the trustworthiness of the cyberspace system, and the feasibility of crime prevention strategies were considered in the Foresight project 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?

In this volume, the contributors demonstrate that addressing these questions within existing paradigms of trust, security and technology does not suffice to alleviate concerns about the potential threats of cyberspace. In many instances, new frameworks taking into account, as far as possible, the distinctive features of cyberspace are suggested with signposts for the kinds of cross-disciplinary research that will be needed.

The issues addressed by the Foresight Cyber Trust and Crime Prevention project are not the only important or relevant ones for the future, but their importance has been signalled by many of those concerned with the increasing potential for identity fraud, changes in the balance between private and public information needs, the role of trust in society and the interfaces between technological innovation and society.[4]

1.2 STRUCTURE OF THE BOOK

This book is organized in four main parts. In Part 1 – State-of-the-Art, we provide a synthesis of the lessons about cyber trust and crime prevention that can be drawn from the existing scientific evidence.

In Part 2 – Future Cyberspace Systems, the focus is on some of the key issues that are likely to influence the future of the cyberspace system including its dependability, architecture and means of handling identities and authentication procedures. Two important areas of technological innovation are the subject of indepth examination – knowledge technologies and the semantic web,[5] and agent-based software deployment.

In Part 3 – Experiencing Cyberspace, we turn to evidence on the ways that people appear to experience cyberspace. The themes in this part centre on risk and trust and the social, organizational and technical challenges of the spread of the Internet and experiences of using it in a variety of social and commercial contexts.

Part 4 – Commentary, comprises a set of three short papers each focusing on a limited theme or issue that emerged in the course of the Foresight project. The first addresses issues around the institutions that influence cyberspace markets, trust and the accumulation of social capital; the second tackles positions on ethical issues and their relationship to cyber trust; and the third offers insight into some of the legal considerations with respect to principles and practices in the digital age.

1.3 CONCLUSION

As the information societies of the 21st century are being constructed, it is increasingly being acknowledged that the whole of the cyberspace system is subject to emergent and unpredictable system behaviour. The contributors to this volume show why developments in cyberspace technologies and the social system are giving rise to new opportunities for crime. Strategies will be needed to minimize these opportunities and such strategies clearly will involve numerous choices. The solutions for improving cyber trust and crime prevention in a future pervasive cyberspace environment will differ from those in use today.

In Chapter 2 we provide a synthetic account of the numerous issues and problems facing those seeking to strengthen strategies for crime prevention. The analysis in Chapter 2 and the state-of-the-art reviews of existing research in subsequent chapters demonstrate that there is a serious deployment gap with respect to the software development methods and procedures used in the construction of the technical components of cyberspace. Improved levels of dependability will require greater attention to the commercial issues that influence customer willingness to invest in more dependable ICT systems and to training and education.

We discuss issues concerning the appropriate means of authenticating identity in the light of changes in the design of secure technologies and in social practices and cultural norms of information assurance. We indicate the way that the development and application of 'criminal opportunity' models can inform future crime prevention strategies and show how the field of ICT forensics is influencing the design of data management tools that will be necessary for evidence gathering.

Perceptions of risk and trust in cyberspace are fundamentally important in understanding the way members of the public appraise risk and uncertainty. We examine these concepts from a variety of theoretical and empirical vantage points. These generally indicate that people's perceptions of risk may be amplified or attenuated depending on a large number of social and technical factors. These factors vary depending on whether inquiries into issues of trust and trustworthiness involve person-to-person, person-to-system or system-to-system trust.

We review developments in software agent-based systems and knowledge technologies and the semantic web to illustrate the tactics for fostering trust that are being considered and social dynamics and learning processes involved in cyberspace risk perception and trusting behaviour. We also consider the ethical issues that inform choices about whether or not to intervene in cyberspace to achieve improved protection against crime.

We consider the economic incentives for investing in the deployment of more trustworthy networks and applications and the interactions between different legislative and self-regulatory approaches that govern cyberspace,

especially in the case of privacy protection and security.

A key conclusion that emerges from our review of the existing scientific evidence is that it is relatively weak in important areas that bear on cyber trust and crime prevention. However, we suggest that critical reasoning can be applied to reach judgments about appropriate strategies for crime prevention and about 'acceptable' and 'unacceptable' levels of the trustworthiness of the cyberspace system.

Collaborative and cross-disciplinary research is needed to harness the considerable breadth of expertise that is available in the United Kingdom and elsewhere. New crime prevention measures will be more effective if they are complemented by such research and by measures that enable people to strengthen their awareness of when to trust and not to trust in the cyberspace system.

NOTES

1 'Research in the wild' is a phrase coined by Michel Callon to distinguish science undertaken in a laboratory from inquiry performed by concerned groups, see Callon (2003: 61).

2 We refer to 'cyberspace', that is, a 'space' in which electronic information processing and communication occur. 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 is constantly changing. Not only are the technologies deployed in many different ways, but the exploitation of them by various social groups differs considerably. For simplicity, 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).

3 Office of Science and Technology, see http://www.foresight.gov.uk/ accessed 17 Apr 04.

4 See Royal Society (2003).

5 Knowledge technologies is a term that is used in the literature and referred to as KT. Developments in semantic web technology are often referred to as Semantic Web or SW, see chapters 5 and 6 for definitions and a discussion.

REFERENCES

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.

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.