

No.005

**Media, Connectivity,
Literacies and Ethics**

**Security Challenges of
Networks: Cyber Trust
and Cyber Crime**

Robin Mansell

March 2006

EDS Innovation Research Programme

Is a collaboration between EDS and leading LSE academics from a range of disciplines researching the determinants of innovation, technology, creativity and productivity and the policies needed to foster them.

The Discussion Paper series features the research of the four teams;

1. Public policy and services (Patrick Dunleavy, Department of Government)
2. Intellectual property, technology and productivity (John Van Reenen, Danny Quah, Centre for Economic Performance & Department of Economics)
3. Media, connectivity, literacies and ethics (Robin Mansell, Department of Media & Communications)
4. Complexity, mediation and facilitation. (Patrick Humphreys, Institute of Social Psychology)

Published by
EDS Innovation Research Programme
London School of Economics and Political Science
Houghton Street
London WC2A 2AE

© Robin Mansell, submitted March 2006

ISBN 0

Individual copy price: £5

Security Challenges of Networks: Cyber Trust and Cyber Crime

Professor Robin Mansell ¹

Department of Media and Communications

London School of Economics

1. INTRODUCTION

The future security of societies that depend increasingly on networks is contingent upon how our complex human and technical systems evolve. New network technologies including the Internet favour fragmentation into many loosely connected open and closed communities governed by many different principles. As the reach of today's networks has become global, they have become the focus of arguments over the values that should govern their development. A key issue is the relationship between trust and crime prevention. Some of the factors influencing the evolution of networks and the feasibility of various crime prevention measures are considered in this note.

The development of networks, or 'cyberspace' as it is sometimes called, raises issues that are fundamental to individual and collective human safety and security. Analysis of the potential threats to human safety and security in a pervasive network 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.

Today's network systems are being created in an environment that embraces interdependent systems of production, consumption, governance and control. This environment is giving rise to new perceptions of risk and to new meanings and interpretations of the security of network developments. People 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 and for private and public sector organisations.

There are many uncertainties about the trade-offs that will accompany human and technical measures to develop a more dependable and secure network system. Introducing legislative and governance solutions may manage risks more effectively, but stifle innovation and competitiveness. It is clear, however, that crime prevention measures are more effective if they are complemented by investment in adequate levels of education and in building awareness.

2. MEASURES FOR ENHANCING NETWORK SECURITY

Crime prevention means reducing the risk of the occurrence of crime and the potential seriousness of crime events that may occur in the online or offline worlds.

The techniques and tools available today make it possible to produce complex computer systems that are reasonably dependable. However, there is a huge ‘deployment gap’, with many organizations attempting to produce complex systems and software using technical and management methods that do not achieve ‘best practice’ standards. Even with today’s technology it is difficult to adapt the methods and techniques available to deploy reliable systems. Unless there is a major change in the way network systems are deployed, the trustworthiness of the underlying infrastructure and of the applications that run on it will degrade. Major or radical innovations in technology often require equally major or disruptive changes in practices of system design and implementation.

Complex software projects are undertaken in order to meet the business needs of an organization or within a contract to be delivered to an external customer. It is vital not only that the users are engaged in the development process from its inception and that the project team has well-defined mechanisms that allow the users to be involved in the project. It is a common experience that project management methodologies with well-defined processes for engagement are not always invested in or trusted.

Identification and authentication within network systems involve objects, whether these are people, devices or digital data. People are not the only ‘actors’ that need to be identified for networks to be trustworthy. Information (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.

Today's network systems are enabling new forms of attack on people and their possessions and the declining cost of technology makes 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. Failure to provide users with the necessary understanding, training and motivation will result in human error and new opportunities for criminal acts.

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. Empirical studies of users of network 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. In the light of growing evidence about the importance of behavioural factors in achieving system security, there is a shift in security management from concern about technical devices to *management* issues. At an organizational level, the most immediate challenge is to integrate security into business processes.

3. TRUST, RISK AND CRIME PREVENTION

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

The need for a trust framework for understanding online commercial interactions has

been recognized. It is necessary to differentiate between situations requiring different types and levels of trust. Trust needs to be a core concern in the design and deployment of technologies and it is now being acknowledged more widely that technical systems can only work as part of a larger socio-technical system. In this context, trust appears to reduce the need for costly control structures, and makes social systems more adaptable.

Crime occurs in many forms in association with network systems. These developments can be addressed in the context of crime prevention strategies through the elaboration of ‘criminal opportunity’ models. The ‘conjunction of criminal opportunity’ model (Ekblom 2004), for example, provides a means of considering the conditions necessary for a crime to occur and the possibilities for prevention. It focuses on the predispositions of potential offenders and on the immediate characteristics of the crime situation – in this case the online and offline situation of users and the systems within which they operate.

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 network systems; others want to alter the design of networks to make inappropriate behaviour more difficult. Different views about the arguments supporting approaches to crime prevention strategies hinge on the extent to which actors are presumed to be rational and are likely to act to maximize their own self-interest. In an environment where there are multiple complete or partial identities, standard assumptions about what motivates actors need to be carefully considered.

4. CONCLUSION

Research yields insights into the way technical innovation is intersecting with human capacities for learning about network system developments. There are uncertainties about the trade-offs that will accompany human and technical measures to develop more dependable and secure systems.

The literature on risk and trust formation and their relationships to the design and implementation of network systems emphasizes the importance of values, reciprocity,

information management and human and technical capabilities.

Table 1 Network systems and 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	Risk amplification
Individual privacy	Collective interest
Liability	Risk and cost
Security	Economic growth and innovation

Source: Mansell and Collins (2005)

Existing research is inconclusive with respect to the implications of interventions by those who seek to minimize crime. Nevertheless, it is clear that:

- improved crime prevention in network systems depends upon a better understanding of human motivations and practices and the way these are embedded within complex systems;
- problems facing crime prevention will not be solved by better technology alone; enforcement of behavioural change consistent with ‘good’ behaviour will mean enabling people to do the ‘right’ thing easily with substantial implications for the usability and cost of technologies;
- trust can be fostered in both technical and non-technical ways; the options need to be considered in the light of studies of risk perception and the actual risk encountered in network systems and in the wider environment;
- crime prevention measures need to receive widespread consent nationally and internationally if they are to be effective; and
- the dependability of future network systems and the extent to which they ensure

human safety and well-being are matters of human choice.

The greatest challenge in the future will be managing the emergent properties and vulnerabilities of network systems in ways that respect changing individual and collective values.

References:

Eklblom, P. (2004) 'The Conjunction of Criminal Opportunity', developed between 2001 and 2004,
<http://www.crimereduction.gov.uk/learningzone/cco.htm>.

Mansell, R. and Collins, B. S. (eds) (2005) *Trust and Crime in Information Societies*,
Cheltenham: Edward Elgar.

Notes:

¹ This paper draws in part on material prepared for the Cyber Trust and Crime Prevision project conducted by the UK Office of Science and Technology Foresight Programme. The views incorporated in this short synthesis of part of that work are not necessarily those of any institution and the author accepts full responsibility for the views expressed and for any errors or omissions. The author thanks all those who participated in Foresight project. Full coverage of the project results can be found at: http://www.foresight.gov.uk/previous_projects/cyber_trust_and_crime_prevention/index.html

EDS Innovation Research Programme
London School of Economics & Political Science
Lionel Robbins Building
Houghton Street
London WC2A 2AE
020 7955 7285
www.lse.ac.uk/eds