[Robin Mansell](http://...)

Network insecurity in an insecure world

Conference Paper

http://eprints.lse.ac.uk

Network Insecurity in an Insecure World

Professor Robin Mansell [1]
Department of Media and Communications
London School of Economics

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. Network communities are subject to highly unpredictable emergent behaviours, making the consequences of efforts to prevent crime very difficult to predict. In some areas, however, there is considerable stability and understanding of relationships within the system to justify action aimed at improving crime prevention.

As the reach of today's networks has become global, they have become the focus of a growing amount of 'research in the wild' and the subject of arguments over the values that should govern their development.[2] A key issue is the relationship between trust and crime prevention in an insecure world. Some of the factors influencing the evolution of networks and the feasibility of various crime prevention measures are considered in this paper.

The continuing development of networks, or 'cyberspace' as it is sometimes called, raises issues that are fundamental to individual and collective human safety and security. The principal technologies considered in this area are those that play a major role in managing human and software agent identities and authenticity, in delivering network system robustness and dependability, in augmenting security and in contributing to information assurance and knowledge management.

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. Much of the information people receive about risk

1

comes from the media and a growing variety of Internet-based sources of imagery and symbols. All of this information is interpreted in different ways, producing consequences that we are only beginning to understand.

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. The importance of network security issues 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.

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 in the process. In addition, no 'future-proof' set of measures can be put in place through unilateral action because the positions of governments, businesses and citizens are changing and are insufficiently clear. However, it is clear that 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 network systems.

MEASURES FOR FIGHTING NETWORK INSECURITY

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 new initiatives to ensure the development of trustworthy technologies. There are similarly divergent views about the need to constrain 'cyberspace' or network developments in order to limit the potential for destructive attack, strengthen collective security and limit privacy invading intrusions.

Technical and possible market developments in the field of pervasive computing and

trustworthy information and communication technology (ICT) systems suggest that some of the technologies are relatively mature, but still evolving. Other technologies are immature, but reasonably predictable, and still others are in the 'blue-skies' research phase. The technologies range from 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.

Crime prevention in this context means reducing the risk of the occurrence of crime and the potential seriousness of crime events that may occur in the online or the offline worlds. The solutions to the evolutionary 'arms-race' involving new technologies will lead to new technical designs, but their feasibility will depend on changing social, cultural, political and economic priorities as well as on a number of ethical considerations. The future use of ICTs will be inextricably bound up with systems that coordinate a large number of technologies within agreed interfaces and standards, which themselves will experience periods of transient stability. These will evolve from generation to generation, as the technology shifts and the players act in various ways that change their motivations and actions.

Trustworthy Computer Systems

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.

System dependability is the ability to avoid computer system failures that are more frequent or more severe than is acceptable. It is not feasible to escape the need to accept some level of failure. 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 factor for the design and construction of a complex computer system – and for the costs of system development and use.

A variety of fault prevention and fault removal techniques is currently in use, but 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 instances, for software faults. However, fault forecasting has limitations with regard to large systems and extremely high dependability targets. The problem of deliberate attacks on networked computer systems and on other major infrastructures by amateur and professional hackers, criminals or well-resourced terrorist groups is already serious. Detecting the onset of such attacks is insufficient to ensure system dependability. Means are needed for maintaining satisfactory service despite such attacks.

Because network systems are increasingly pervasive, they are being used in the design and testing of new systems and in 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 and those used for evidence gathering in support of judicial processes. The latter must be at least as trustworthy as the end-user system.

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 customer is engaged in the development process from its inception and that the project team has well-defined mechanisms that allow the customer to be involved in the project. It is a common experience that project management methodologies with well-defined processes for customer engagement are not always invested in or trusted.

Large software projects are not unusual in having changes imposed upon them by external factors and frequently the basic assumptions on which the projects are based are not examined. In such cases it may be necessary to stop the project or re-design to accommodate these new developments. Ideally, buyers of such projects should insist on careful monitoring and use educated and experienced people in the design and implementation of large software projects to minimize risks.

Identification and Authentication

As the automation of business and the use of electronic forms of communication increase, individuals must find 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 by email, they have 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.

Identification and authentication within network systems involve objects, whether these are people, devices or digital data. There are three ways for users to authenticate themselves to a system - a computer, a network or another individual: i) something they own; ii) something they know; or iii) something they are, i.e., a personal characteristic. Use of combinations of at least two is common. Typically, the 'something owned' might be a token. If that token such as a smartcard, has some form of processing capability, 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, which might also be used as an activation process for a smartcard.

It is now common for a smartcard to have encryption capabilities and to contain cryptographic keys. The authentication process may involve sophisticated protocols between the card and the authenticating device. However, before any of these techniques can be used, there must be an identification of the users to ensure that they have been given the correct object or knowledge or that the characteristic being associated with them is theirs. Most commonly used authentication techniques assume that there has been an initial, accurate identification and rely on that assumption.

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. The only authentication techniques that attempt to authenticate a user directly are biometrics. 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.

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.

Although there are many mechanisms for authentication, there is no single mechanism for usable authentication. The usability of any authentication mechanism depends on the nature of the task to be performed. Failure to provide users with the necessary understanding, training and motivation will result in human error. Users are often left to make a choice between complying with security regulations and completing a task.

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.

The problems associated with establishing identity are often ignored in discussions relating to 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 a person's identity has already been established elsewhere. Each new process is merely endorsing the old one. There are numerous examples of where the ability to impersonate someone in the registration stage implies the ability to steal that

person's identity and impersonate the person for life.

In addition, forensics in the area of network security and crime prevention is in its infancy. It is mainly involved with data held on hard disks in PCs, personal data assistants and other memory devices. These are used by criminals for some activities and, when captured, the data on the devices provides evidence. In order to provide such evidence, all entities – documents, computers and disks – have to be identified and authenticated. The strength of the process of authentication is critical in the case of digital evidence. If a document such as an email, 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, when and on what 'machine', is essential. The quality of the proof will rely not only on the data, but also on the veracity and traceability of the process by which the data are managed.

In summary, future network systems will be constructed out of multiple existing systems and will also need to be highly adaptable. Most will embody human beings. The successful design and deployment of such systems is a major challenge that calls for expertise and socio-technical, as well as technical, research. Cross-disciplinary approaches are essential if any inroads are to be made in this field.

TRUST AND RISK

Many assumptions about trust and risk in network systems are made by technology developers and users. The trustworthiness of the 'space' implemented by the use of network systems will only be enhanced when we have a deeper understanding of how knowledge can be managed throughout its life cycle by people and software agents, interactively and collaboratively. This process has to be managed in such a way that outcomes of transactions and interactions are reasonably predictable and are perceived as being acceptably safe. To achieve this, it will be necessary for the barriers to criminal or socially unacceptable use of network systems to be sufficiently high to minimize opportunities for unpredictable interactions associated with behaviours that are not socially valued.

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 network systems. The way the public sees experts and regulators also may influence how risks are perceived or actually experienced are interpreted.

Insights into the perception of risk can be drawn from theories in cognitive psychology, psychometric research, and studies of the relationship between emotion and risk perception. These insights need to be examined in the light of people's perceptions about the riskiness of network systems. 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 events. Social meaning must be expected to influence appraisals of a perceived threat or an uncertain event.

Trusting in Networks

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. It is clear 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 increasing. 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.

Trust can be seen as 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 are available. For instance, 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 focuses on the institutional structures – laws, rules, norms, and standards – that are imposed on market players and govern their interactions. 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'.

Economists focus on the costs of breaching trust as the principal motive for maintaining it. Trust serves as a 'lubricant' in markets, reducing transaction costs and assuring something closer to perfect competition. The institutional framework for 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, that is, trustworthiness. Choices that are made about whom to interact or play with, and whose expectations to fulfil, disappoint or ignore, determine the 'network structure'. In game theoretic contexts, it is relevant to consider how the design of the game itself embodies trust, especially where contracts may be incomplete. Trust is essential to the functioning of the norms and standards that allow markets to function.

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 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 which establishes a structure for negotiating the liabilities arising from interactions. Aligning the institutional rules of network systems with the tendencies of a network may improve efficiency. But because it is possible for the independent actions of one member of a network to compromise the interests of others, networks may need stronger rules for exclusion or for imposing sanctions on participants that breach the trust of others.

A problem confronted by 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 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 such that 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).

Proximity or 'experience' with the Internet is one of many factors that could play an important role in perceptions of appropriate levels of trust. Research conducted by the Oxford Internet Institute has highlighted issues concerning trust in a preliminary way. A surprisingly small percentage of Internet users reported bad experiences. Understanding relevant social and institutional dimensions of trust should be a key priority in addressing the way these technologies affect trust, crime and related issues.

Crime Prevention Strategies

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, 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. See Table 1.

Conjunctions of criminal opportunity occur 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. Preventive interventions can act by interrupting, diverting or weakening any of these causes.

Table1 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 (2004).

This approach could be extended to examine the organizational contexts and behavioural characteristics that are most likely to give rise to criminal opportunities associated with network systems.

Views are divided about the ethical justification for interventions in network systems that seek to limit the potential for crime. 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 requirements or justification for changes that might limit the scope for anonymity.

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 moral arguments supporting different 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 scrutinized.

CONCLUSION

Research evidence 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. Some of these trade-offs are summarized in Table 2.

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 2 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

Existing research is inconclusive with respect to the implications of interventions by those that seek to minimize crime. There is a need, therefore, to consider the ethical positions associated with crime prevention measures and to draw inferences about their impact. 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 will 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:

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.

Ekblom, P. (2004b) 'The Conjunction of Criminal Opportunity', developed between 2001 and 2004,
http://www.crimereduction.gov.uk/learningzone/cco.htm accessed 2 Dec 05.

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

2 '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).