WWW.EFMN.INFO The European Foresight Monitoring Network

Cyber Trust and Crime Prevention 2018

Foresight Brief No. 10

Authors: Jane Jackson, Foresight Directorate, Office of Science and Technology jane.jackson@dti.gsi.gov.uk

Sponsors: The Home Office

Type: A national single issue foresight that considers the science, technology and socio-economic fields that affect or are affected by the issue.

Organizer: Foresight Directorate, Office of Science and Technology www.foresight.gov.uk

Duration: March 2003 to June 2004 **Budget:** €650,000 **Time Horizon:** 2018

Purpose

The aim was to take an independent and objective look at the subject of the vulnerability of ICT and using the best knowledge available explore the applications and implications of next-generation technologies on this issue.

The challenges of the foresight exercise were to:

- Set out visions of the future, define a range of possible outcomes, identify possible drivers, opportunities and threats, barriers to progress, and models for decision-making,
- Create networks of scientists, business people and policy makers who can act on the findings to influence the future,
- Set out some key challenges and engage those who can take them forward.

The Challenge of Trust and Security in a Cyber World

The UK Foresight programme is formed of a rolling programme of focused projects. Cyber Trust and Crime Prevention was a topic suggested by a workshop of eminent scientists which then received support from UK government and academia. More generally, they realised that ICT was increasingly integral to the functioning of modern society and therefore needed to be trusted by the users and not be vulnerable to attack by crime particularly in view of the need to keep pace with the rate of development of the technology.

The objectives of the project were to:

- Explore the challenges facing policy makers, businesses and the public by the rapid development of ICT if there is to be future trust in cyber systems,
- Contribute to the framing of the debate to help ensure the UK maintains its position as a major ICT player, that new technologies can be used to create wealth and to improve the quality of life as rapidly as possible,
- Enable technology to be used to reduce crime, and
- Investigate the extent to which technology introduces new forms of crime, or extends the scope of existing crimes.

The **EFMN** is financed by the **European Commission Directorate General for Research** as part of a series of initiatives intended to provide a **Foresight Knowledge Sharing Platform** for foresight practitioners and policy makers in the European Union. More information on the EFMN and on the Foresight Knowledge Sharing Platform is provided at **WWW.EFMN.INFO**

The Foresight Approach

The project was overseen by a stakeholder group chaired by a minister from the Home Office with the membership drawn from business academia and government.

The mechanics of the project were carried out through a series of workshops, firstly to define the scope of the project. The scope formed the basis for the commissioning of state of the art science reviews, which in turn fed into three sequential workshops picking up on particular themes derived from the reviews and from the outputs of the previous workshop. A sub group looked at what future technological developments were likely to occur. A period of analysis and synthesis of the results led to the development of three scenarios set in 2018. These were in turn explored in gaming seminars involving participants from the public sector, business and research communities to look back from 2018 to envisage what could be done today to make these scenarios more palatable.

Diagram 1 below shows the inter-relationship between the different parts of the process.

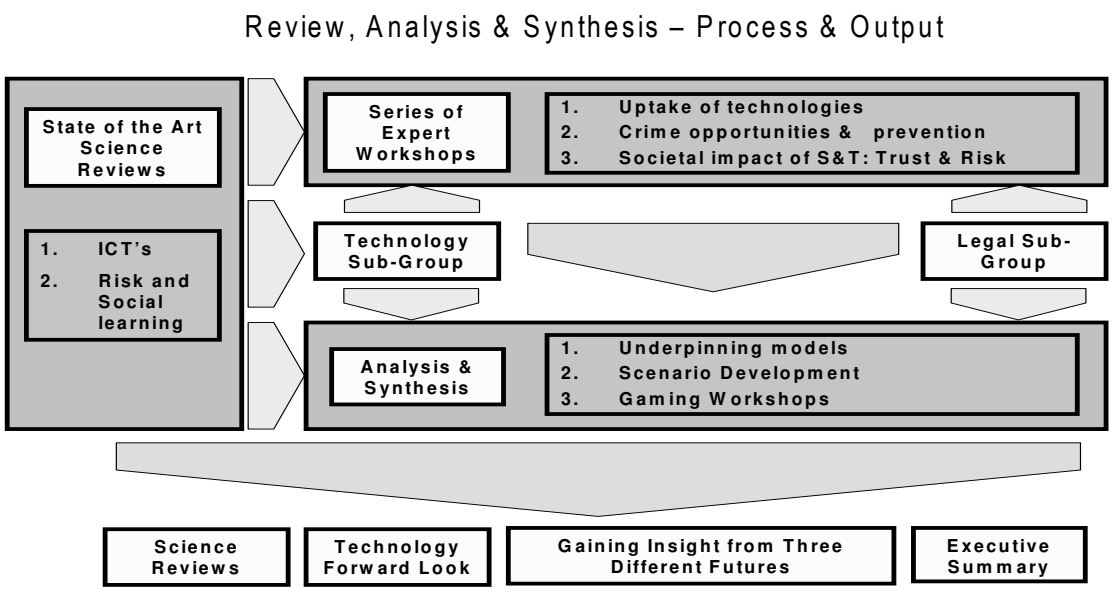

Diagram 1: A representation of the process undertaken in the Cyber Trust and Crime Prevention project

When the project's findings were published an Action Plan was drawn up to apply the outcomes of the project and to explore the implications of the project's findings. The stakeholder group will meet in autumn 2005 to assess progress against the Action Plan.

Future Visions

How the Risks May Change

We are moving steadily towards pervasive and ubiquitous computing: everything we buy and wear may be electronically tagged and connected. There will be huge data sets, intelligently mined by autonomous and intelligent software. Whilst technology will bring large benefits there will still be risks.

There will be a migration from the internet infrastructure to 'utility computing'. These services will not be confined to the home and personal digital environments, but will be created with wearable technology allowing people to be connected at any time and in any place. Applications and their content will be automatically tailored to the user.

As more systems are developed and integrated there is a risk that the complexity and hence vulnerability of the systems will increase. Vulnerability will be both in terms of risk of failure of parts of the system and more opportunities for crime.

The rapid pace of innovation and adoption of new systems makes it increasingly difficult to keep up with the new risks. This means there could be increasing incidents of spotting and reacting to new crime opportunities long after they have created the damage.

Perception of risk is a significant factor which affects whether people take advantage of the opportunities offered by the new cyber-world. Managing this is a key aspect of any response to management of future risks.

How the World Might React to the Changes in Risk

Three scenarios helped to explore how society might react to these changes. The scenarios were based on different approaches according to who takes responsibility for security and the consequent willingness to share information with others.

The three scenarios were:

- **Frog Boiler:** We carry on as we are indefinitely, with an unclear delineation of responsibilities across individuals, business and government and limited access to information on the activities of individuals in cyber space;
- **Touch me not:** Individuals do not allow others to know what they are doing but accept that they should take more responsibility for their own security;
- **Knowing it all:** Individuals are content to let government have more access to what they do in the digital world but in return expect business and government to police the risks.

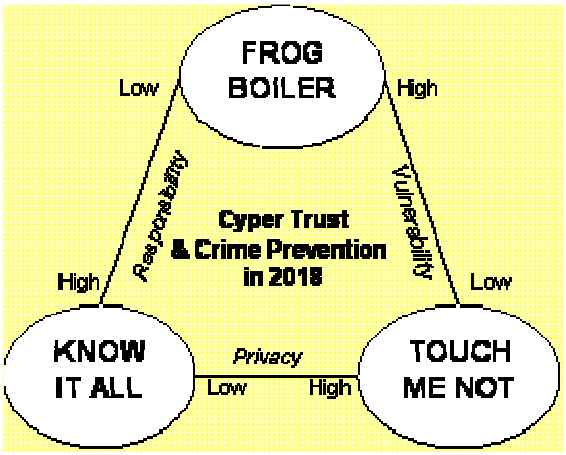

Diagram 2: The three scenarios are set on the outer edge of the future possibility space and are used as a tool to investigate the key factors that may affect cyber trust and crime prevention

What we should do now to Respond to Emerging Challenges

The project considered what might enhance the trustworthiness of complex systems in the future, what might enhance cyber trust, whether new types of criminal opportunity associated with ICT could be reduced, what were the implications for future research.

The participants of the workshops identified the following elements of a response to the emerging challenges and risks:

- **New digital forensic tools** to automatically scan for potential problems and assign provenance in an auditable way. As ICT becomes increasingly pervasive both context and data provenance will be increasingly key. As data storage increases so will the need for improved digital forensics and evidence processes.
- **New structures which allow government and business to identify and design strategies to respond to the new risks.** The challenge for the future is to be sufficiently fleet of foot to respond to the quickly changing challenges. For example, to consider the implications of developments in data-mining and autonomous agent software.
- **New language and frameworks** are required for a response which can be applied in a quick, flexible way to new challenges as they arrive. One of the delays in responding to risk is often labeling it, getting a common understanding of it and then working out how something new fits in with our current systems of risk management.
- **Design-out crime but design-in usability.** Although cyberspace is new, the behaviors that are important in understanding criminal opportunity are largely the same. Opportunities arise from the complexity of the technology, particularly the growing 'system of systems'.
- **Continue to build international collaboration to respond to the risks.** Cyber crime is a global issue and international cooperation will be needed to address it, with ethical principles guiding the debate. A need to improve international law enforcement cooperation and further develop international standards was identified, including harmonization of international data protection legislation.
- **Develop a stronger partnership between government and business to improve law enforcement capability.**

The impact upon the legal and regulatory system needs to be explored further. There is acceptance that some personal data needs to be collected for effective law enforcement, but that there should be strong independent monitoring and audit of public sector data use.

- **Develop solutions to improve trust:** The perception of risk in cyberspace is largely based on experience, but there are a range of socio-economic variables that impact upon people's behavior. Identity, security and privacy are all factors that affect how trusting people are. Possible solutions to improve trust include better information for the user about technologies and their risks, together with dialogue between government and business.
- **Decide how we should use the quickly developing technologies for identification and authentication:** For example, initial identity enrolment must be consistent and accurate. With rapidly accumulating data there is an absolute requirement for clear provenance of information objects. Usage is not just affected by flaws in technology, but by individual behaviors and cultural differences.

The project considered what might enhance the trustworthiness of complex systems in the future, what might enhance cyber trust, whether new types of criminal opportunity associated with ICT could be reduced, what were the implications for future research.

A Clear Governance Structure

Trustworthiness has not been seen as a major issue in the development of new ICT over the last two decades, especially when compared to functionality and users generally welcomed new applications. However, some participants in the project took the view that current models of proprietary systems were at odds with modularity, stability, simplicity and open scrutiny, which were likely to become increasingly important in the future and were essential for the creation of highly trustworthy systems. In that case, the UK and EU might create competitive advantage by establishing effective standards in areas such as traceability and provenance that could then be adopted elsewhere. Without more action to reduce the impact of new vulnerabilities the risks created might be one of the biggest brakes on the deployment of new capabilities.

The gaming seminars realised that for those looking to enhance trust and the use of ICT based services, there is a need for a clear governance structure to detect and react to abuses of failures, a belief that the issues for the criminal justice systems that are raised by the need to collect and use digital evidence are sufficiently difficult that they are not capable of satisfactory resolution by 2018.

The structures for dialogue between government parties will need to evolve in the future to allow quicker feedback on identifying and responding to potential criminal opportunities. Several of the project's stakeholders will use the project's findings to explore these issues in more detail.

The main areas for future research are the social amplification of risk, criminal opportunity models, assessment of impacts on privacy, dependable software engineering and digital forensics initiatives.

Sources and References

All the above information is drawn from the Foresight Cyber Trust and Crime Prevention reports which are available at www.foresight.gov.uk