Government
Office for
Science

Foresight

Cyber Trust and Crime Prevention

Mid-Term Review

November 2005 – January 2009

Contents Page

Executive summary

Project background
Combining an independent review of the scientific evidence base with an ambitious, 15-year forward view, the Foresight Cyber Trust and Crime Prevention (CTCP) Project (the Project) was published in 2004 and sponsored by the Home Office. The Project considers how Information and Communication Technology (ICT) risks may change and how society might react to these changes.

This mid-term review (the Review) assesses the impact that the Project has had on its key stakeholders in government, the third sector, and elsewhere and considers some of the factors that may have influenced this.

The Project found that social, business and technological systems are becoming more complex and interdependent, making it difficult to anticipate and address new threats. In particular, the Project argued that technology alone will not provide the solution, thereby requiring improved training, education and, especially, governance. Of central importance to the Project was the issue of trust - in security systems, in data handling and in data storage – which called for new forms of governance and better industry-government communication to identify and prevent new forms of crime as they develop.

In 2005, the Project's High Level Stakeholder Group was reconvened and chaired by the Project's sponsor minister in order to conduct a One-Year Review of post-launch progress. This mid-term Review and impact assessment marks the final phase in the Project's formal life-cycle.

Overview of impacts
A broad survey of expert stakeholder opinion of the Project's impact by the Foresight Follow-up team indicates that the Project achieved better impact in some areas (Research Councils, academic research, professional associations and learned societies) than in others (government departments, business and industry, and internationally).

Principal impacts include the Cyber-Security Knowledge Transfer Network (KTN), developed by the Technology Strategy Board (TSB), BT, and QinetiQ, among others. The Project has also informed the Home Office consultation "Protecting the public in a changing communications environment" and the work of the Council of Science and Technology and the Forensic Science Pathology Unit.

Indirectly, the Project has shaped consensus and raised the profile of the challenges posed by cybercrime. And, since 2004, the Research Councils have credited the Project, directly or indirectly, with influencing research funding in the region of £60m. This included three further calls for proposals which have led to, among other things, funding for 30 research projects, three networks, and six feasibility studies across the fields of cyber crime security research.

Particular impact has also been achieved in academia where, since the 2005 One-Year Review, there has been a wide range of activities attributable, in whole or in part, to the Project. These impacts include the creation of a valuable interdisciplinary network as well as informing the development of teaching courses, research programmes and publications.

In business, the Project was instrumental in developing the ‘Trustguide’, a joint venture between British Telecom and Hewlett Packard and Government Office for Science (then the Office of Science and Technology). 0This initiative picked up from where the Project finished and produced guidelines on enhancing cyber trust and was aimed at all those researching, developing and delivering ICT.

The Project, however, was not without criticism, particularly with regard to a perceived lack of government leadership in drawing on the Project findings – a criticism brought into sharp relief after the series of data handling problems, prompting the Information Commissioner, Richard Thomas, to dub 2008 as “the year of data breaches and data losses”[1]. Several issues were identified by Review contributors, particularly the opportunity for the more focused and sustained public sector leadership and that the Project’s 15-year future timescale was too ambitious. However, many observers admired the willingness to take on such a challenging, comparatively long-term view in the fast-changing ICT sector.

An important criticism of the Project was that the research and findings crystallised a year too early (2003), thereby inadvertently missing a radical change in the nature of cybercrime, from hacking high-profile targets for kudos to surreptitious hacking of an almost unlimited supply of small targets for value (of goods and services). Consequently, while the Project’s key themes are still relevant, some of the findings may be somewhat misaligned with the present reality.

However, despite these perceived shortcomings in the Report and its impact, it is clear that the Project has significantly influenced – and continues to influence – the ICT sector. Moreover, given the damage to public sector credibility in handling data following “the year of data loss”, there is recent evidence for the Project’s continued relevance, which creates potential for revisiting its findings. For instance, in 2009 alone, the Project was credited as a “significant forward look in the field of cybercrime”[2], influenced £3m of research funding[3], and informed two Home Office initiatives[4].

[1] 17th RSA (information security) Conference, London, 29 October 2008; www.ico.gov.uk/upload/documents/pressreleases/2008/rsa_speech_oct08_final.pdf (accessed 28 November 2008)

[2] NESTA (July 2009) *Crime online: cybercrime and illegal innovation* NESTA, London, p11, 62.

[3] as part of the EPSRC- Global Uncertainties theme, 'Detecting Terrorist Activity', July 2009.

[4] CTCP PROJECT influenced Home Office work on Privacy and Security (April 2009) and its “Protecting the public in a changing communications environment” consultation (July 2009)

1 Introduction

Foresight was recast in 2002 as a programme of major in-depth studies examining major issues up to 80 years in the future. These projects combine the latest scientific and other evidence with futures analysis to tackle complex issues and help policymakers think more systematically about the future.

Cyber Trust and Crime Prevention (CTCP) was the fourth Foresight project and, as such, was one of the early studies in the new Foresight model. Although all Foresight projects are different in their methodologies and approaches, CTCP was important in helping shape the Programme during its formative stage.

The CTCP project (the Project) was sponsored by the Home Office and reported in June 2004. It provided a robust evidence base which aimed to inform policy making, strategic thinking, research and investment in technology development to address the challenges it raised. This mid-term review (the Review) explores the activities of government and other organisations which have been informed by the Project findings.

Achieving and recording impact is an important aspect of all Foresight's major projects. To this end, Foresight routinely undertakes a formal review of projects' impact during the year following their launch and, in CTCP's case, this was published as the 'One-Year Review' (OYR) in 2005. However, it has become increasingly apparent that the impact of many of Foresight's major projects plays out over a longer time scale. Therefore, Foresight is conducting a series of mid-term (3- to 5-year) reviews, of which this is one, to explore these impacts.

In order to help projects achieve impact, Foresight has set aside resource to disseminate reports and their findings and to catalyse action. This 'Follow-up Team' works with government and other stakeholders to help ensure that projects are used to inform their activities, in particular in the year following publication but also to capitalise on specific opportunities which arise in the longer term. This Review is a record of some of those impacts. However, it is not intended to be comprehensive as impact will often be indirect or intangible and not clearly attributable to the Report.

The Review provides an overview of the Project, its main findings (chapters 2 and 3), and a summary of the OYR (chapter 4). It also sets out the Review methodology; the Project's impact by sector in particular, within the academic and research communities and, to a lesser extent, government departments, and business; and conclusions (chapters 5, 6 and 7).

It is important to note that the Project does not make policy recommendations as such; rather it seeks to develop the evidence to inform them, as do all Foresight reports.

2 Project overview

The Project was motivated by the fact that Information and Communication Technology (ICT) has brought, and will continue to bring, great benefits to society, the economy, and the individual, both in the UK and worldwide. However, as ICT reaches further into our public and private spaces, it raises complicated, uncertain and interdependent issues. How do you know with whom you are dealing when you send an email? How do you want to be able to vote or to receive benefits, health care and financial services in the future? How can we use these technologies to reduce crime and what should we do to limit the crime opportunities they may offer? What standards of protection should we apply?

- “Cyber trust” derives from perceptions of the purposes of ICT-based systems, and trust in how they are built and used in relation to their purpose. Much of trust in cyber systems is about system functions and roles in relation to ordinary life, and our perceptions of what it means to be citizens, customers, community members and individuals.
- “Crime prevention” – guarding against criminal exploitation – is only one aspect of creating trustworthy citizens. Just as reducing crime, whether it is physical crime or cyber crime, is only one of the many potential uses of ICT systems. The Project addresses some of the broad issues in relation to trust, but gives special emphasis to those raised by crime prevention in order to avoid losing some of the further potential benefits that these technologies can clearly bring.

The Project explores the underlying scientific evidence, the technologists’ views of what might be possible and, using socio-economic input, looks 15 years forward to explore how the risks involved in the use of ICT might change and how society might react.

The Project covered issues such as:

- Identity and authenticity
- Surveillance and security
- System robustness
- Information assurance

It also explored the basis for effective interaction and trust between people and machines.

Foresight began the Project with a comprehensive, independent review of the relevant scientific evidence for current and potential technological capabilities and recent analytical insights from the social sciences and humanities. Working with RAND Europe, the team used this evidence as the basis for the development of three scenarios of how future cyber risks might be managed. Stakeholders reviewed the scenarios to identify the issues that the UK should consider to minimise future cyber crime risks.

3 Key findings

The aims of the Project were to explore the application and implications of next generation ICT. The report looked at:

- How the risks involved in the use of ICT might change over the next 15 years; and
- How society might react to these changes in risk; and

Key points are:

- The pace of technical, social and business change makes it difficult to anticipate and respond effectively to new vulnerabilities in ICT systems.
- There are no purely technological solutions to protect against the ever-present threat of cyber crime that do not also require a significant concomitant change to how the people and businesses understand and use ICT. Moreover, as social-networking and technical ICT systems become more complex and interdependent, it becomes harder to predict how ICT systems might fail, or what the consequences of failure might be.

Therefore we will need:

- New forms of governance to establish systems that are trustworthy and trusted;
- Better mechanisms for business/government dialogue to identify and respond to new criminal opportunities, and to find new ways to prevent existing forms of crime; and
- New forms of training and education, for IT professionals, suppliers and users.

To deliver security, wealth creation and other public goods it will be essential to consider technological capabilities as part of social systems, including drawing on emerging understandings of risk and social learning.

The project developed three scenarios for 2018, including very different (but self-consistent) sets of assumptions about the allocation of responsibilities for security, privacy and liability across government, business and civil society. The scenarios can be used to explore the implications of today’s choices in these areas.

The Project homepage, including Project outputs, is available here: www.foresight.gov.uk/OurWork/CompletedProjects/CyberTrust/ProjectHome.asp

4 Summary of One-Year Review (2005)

The One-Year Review (OYR) assessed the impact of the Project over the year following its publication. The OYR sought to determine where and how the Project had impact and to identify the scope for further action.

In 2004, Foresight had little in the way of a post-launch follow-up resource, so the Project was primarily taken forward by the Project's expert panel and by the momentum developed during the Project's developed. The Project's findings were disseminated to other government departments and entities (particularly Home Office and Cabinet Office) through a series of expert-led workshops, specifically tailored to each group such as the workshop on offender tracking for the Home Office.

Furthermore, the Research Councils launched a number of Project-related funding proposals and the ICT sector undertook a number of initiatives, from seminars and briefings on the Project to the Hewlett Packard and British Telecom joint-led ventures that led to the Cyber-Security Knowledge Transfer Network and the Trustguide Project, which figure later in this review.
The One-Year Review was published in November 2005, http://www.foresight.gov.uk/OurWork/CompletedProjects/CyberTrust/CTCPOneYearReview.asp

5 Methodology

Early analysis for the review indicated that the sector had changed significantly in the four years since the Project launch in 2004. The particular challenge posed by these developments was the identification of threads of activity in the current landscape that could be traced back to the Project.

Review methodology
The commitments made both in the project Action Plan and the impact set out in the OYR were examined and taken as a starting point for the Review.

- Committed to soliciting a wide range of views, the Review identified and evaluated more than 230 experts including the 18 members of the Project Advisory Group, the nine CTCP Science Review leaders, and around 200 stakeholders from across government, academia, the third sector, and industry;

- Of these, approximately 140 individuals were contacted for contributions to the Review with a 30% participation rate, data being gathered via email, telephone, and face-to-face interviews;

- In December 2008, the initial findings were discussed with Professor Brian Collins, Chief Scientific Adviser to both the Departments for Transportation and Business (DfT), Innovation and Skills (BIS), who led the Project's original Advisory Group and who provided useful insight and further leads;

- In order to ensure that opinions were as candid as possible and to reflect the wishes of anonymity of several contributors, all contributions have been anonymised.

For example, one commentator from the financial sector observed that the Project was an unwitting victim of bad timing, arguing that, as the findings were beginning to crystallise before publication, the landscape upon which the evidence was predicated was undergoing a significant shift, explained below.

One academic also identified this problem remarking that the Review "will be difficult as the problem with 'blue skies thinking' is that some of will prove to be wrong or ahead of its time. We've moved on from the hacker craving recognition to a new crime environment typified by stealth, such as phishing and new technologies, each of which provides a new area of opportunity for criminals". The phenomenon of stealth was not included in the Project, in which – unlike the old, fragmented landscape "script kiddies" and "black hats" that sought to achieve high profile security breaches of prominent web-sites – highly organised cyber-criminals (often located overseas) avoid detection at all costs in order that they can maximise their profit from their theft of personal data, bank details, etc., creating "cloned" credit cards, among other instruments.

Clearly, in an technology sector that is said to look ahead generally no further than six months to a year because of the constantly shifting landscape, the Project's 15-year time horizon was very challenging. However a number of commentators remarked that the Project had been a useful attempt in taking the long-term view. For example, NESTA's report on *Crime online: cybercrime and illegal innovation*[5] cites the Project as "a notable exception" to the general lack of cybercrime innovation studies and one of only two examples of "significant forward looks in the field of cybercrime").

[5] NESTA (2009) *Crime online: cybercrime and illegal innovation* NESTA, London, pp11, 62. http://www.nesta.org.uk/library/documents/crime-online.pdf (accessed 17Jan10)

6 Impact by sector

a) Government departments

The Project's most significant and lasting impact on government department-led activity has been through the Department for Business, Innovation, and Skills/Technology Strategy Board's Cyber Security Knowledge Transfer Network[6], which is still active and thriving, producing a series of continuing initiatives on privacy and consent issues (including a joint, £10M research programme with ESRC and EPSRC, announced in March 2008)[7].

Some early impact was also achieved across a number of government departments through informing current initiatives and disseminating findings through four, expert-led Project workshops. Project experts and research guided the Council of Science and Technology's (CST) discussions on privacy and trust in the production of their report[8]. The Forensic Science Pathology Unit (FSPU) has worked with the Project findings in developing its work and, under the CONTEST arena[9], issues of ICT security are part of that agenda. More recently, in 2009, the Project informed Home Office work on privacy and security as well the consultation on the "Protecting the public in a changing communications environment".

However, the Review concludes that - with the notable exception of the Cyber Security KTN – the Project has not achieved satisfactory impact with government departments, particularly given the data security problems of 2008 (although the Review appears to have inspired a flurry of interest within the Home Office in 2009). After some initial interest and "quick wins" in the first year, following the Project publication, the Project appears to have been largely put to one side by government departments.

There are a number of reasons why lasting impact may not have been achieved or why verifiable impacts may have been "lost". These reasons include:

- Challenges in engaging officials regarding a four-year old report;
- High rates of staff turnover within and among departments resulting in loss of corporate knowledge of the Project;
- Changes in departmental policy priorities;
- Changes to the machinery of government; and
- (Then) lack of Foresight resource for follow-up activities

The main culprit seems to be staff turnover. Few of the lead departmental contacts from the Project's publication were still in the same post or in the same policy area four years on and most, if not all, successors to these posts

[6] www.ktn.qinetiq-tim.net/index.php; the KTN is managed by QinetiQ

[7] http://www.epsrc.ac.uk/CMSWeb/Downloads/Publications/Corporate/Scorecard2008-11.doc

[8] *Better use of Personal Information – Opportunities and Risks* (Council of Science and Technology, November 2005)

[9] Established by the DfT in 2006, CONTEST is "the first cross-government counterterrorism strategy and cross-government counter-proliferation framework".

had no knowledge of the Project and little time for – or interest in – reviewing it.

The lack of resource for Foresight Follow-up of the Project is also a significant factor, meaning that not enough attention was invested in disseminating the Project's findings after the launch. This problem is now being addressed by a dedicated team to develop Follow-up activities as an important part of project structure and impact.

b) Research Councils

Although the Research Councils' engagement with the Project started relatively tentatively with an undertaking to hold a meeting with the relevant research programme managers, the Project's influence has spread significantly within the Councils to become one of the Project's chief impact areas – particularly through responsive mode funding applications.

The OYR noted that the Research Councils were preparing a funding proposal for a cross-council network to continue that formed by the Project, and that electronic crime prevention had been raised to a "priority theme" and allocated £0.7m (EPSRC) to related projects chosen in the 2003 call for proposals.

Since 2004, the Research Councils have credited the Project, directly or indirectly, with influencing research funding in the region of £60m. These developments included three further calls for proposals which have led to, among other things, funding for 30 research projects, three networks, and six feasibility studies across the fields of cyber crime security research[10].

A Research Councils' official observed that RCUK,

> "continues to fund proposals relevant to cyber crime and security through various routes and the decisions we make can and do draw on the CTCP Project's outputs… Responsive mode funding continues to be allocated to proposals on the basis of research quality and impact. The more impact that a proposal can show, the better its chances of being funded, and activities like Foresight help to make the case for why a proposal has impact, hence increasing the likelihood of a proposal being funded. This is an indirect, but very real, effect."

The Research Councils have identified the following examples of the Project's influence on funding:

- A cross-council, ESRC-led initiative, "*Global Uncertainties: Security for All in a Changing World***"** programme. The Project produced some of the evidence required to identify, scope, and agree funding for this programme;

[10] However, not all of these projects appear to be related specifically to the CTCP Project's key themes

- Leading on from the work done in the Project, issues of cyber security featured in a IDEAS factory (EPSRC) event held as part of the Global Uncertainties theme entitled *'Detecting Terrorist Activity'*, with at least £3m committed in July 2009;

- The Interdisciplinary Research Collaboration in Dependability (DIRC) addressed the dependability of computer-based systems. Started in 2000, DIRC was a six-year programme with academics from five universities. Two new projects (InDeED and TrAmS) will take the DIRC ideas forward:

  - InDeED[11]: a long term, four year research project that started in July 2006. The aims of InDeED are to develop knowledge, methods and tools that contribute to the understanding of socio-technical system dependability, and that support developers of dependable systems;

  - TrAmS[12]: Trustworthy Ambient Systems, focussing on the trustworthiness of ambient systems ("in which mobile computing devices and software agents form ad hoc groupings, sharing data and services"), encompassing both dependability and the evidence that a system is dependable;

- £20m of funding was announced by EPSRC/TSB/BBSRC (20 November 2008) to establish two Innovation and Knowledge Centres (IKCs), one of which will be established (with at least £10m over five years) at Queen's University Belfast (QUB) and will specialise in cyber security[13];

  - The QUB IKC will work on the security of the UK's information architecture and the trustworthiness of information stored electronically;

- ESRC, EPSRC and the Technology Strategy Board launched a joint, £10m funding call on privacy technologies, *"Ensuring Privacy and Consent*"[14] , starting with £5.5m funding for three initiatives[15]:

  - VOME: an initiative aimed at visualising users' privacy and consent issues to inform software and hardware development

  - Privacy Value Networks (pvnets): developing ways to value privacy in order to inform actuarial calculations of risk and impact assessment on personal information

[11] www.indeedproject.ac.uk/

[12] www.csr.ncl.ac.uk/projects/projectDetails.php?targetId=223

[13] www.epsrc.ac.uk/PressReleases/£20Million.htm

[14]http://www.epsrc.ac.uk/CMSWeb/Downloads/Publications/Corporate/Scorecard2008-11.doc

[15] http://www.innovateuk.org/content/news/new-research-projects-help-to-ensure-privacy-of-da.ashx

    - EnCoRe: a digital rights management (DRM) tool for individuals to control the use, storage, and sharing of personal data;

- Helping define programmes such as the joint EPSRC/ESRC/AHRC *"Countering Terrorism in Public Places"* research programme[16], informing the development of government work on many aspects of security;

- Forming part of the case for funding the RCUK, cross-research council programme, *Digital Economy*[17] which aims "to realise the transformational impact of ICT for all aspects of business, society and government and to fund research relevant to cyber security". The EPSRC is working closely with ESRC, MRC and AHRC to deliver the programme, which includes £36m to fund three, new cross-discipline digital research hubs[18] and up to £30m to fund up to five doctoral training centres[19]

c) Academia

In view of the fact that most of the Project experts were academics, it is not surprising that the Project achieved particular impact in the academic world – notwithstanding the fact that academic articles have a longer publication trajectory that precluded their capture in the OYR.

Since the 2005 OYR, there has been a wide range of academic activities attributable, in whole or in part, to the Project. These impacts can be divided into four, broad categories: General; Publications; Teaching; and Research.

i) General

According to feedback from various contributors, the Project led to a number of indirect influences on the academic sector. These impacts are somewhat intangible, but are worth capturing as they suggest that many of the Project's impacts are difficult to assess or measure.

For example, by bringing together much of the existing evidence on the subject and shaping an expert consensus, an important interdisciplinary network was formed that continues to be valued by many of those who participated. This network was consistently cited as one of the Project's most useful legacies. It has led to continuing collaborative research and publications and has enabled experts from one academic discipline to gain further insight into their work through exposure to ideas from other disciplines.

[16] www.epsrc.ac.uk/ResearchFunding/Programmes/BetterExploitation/Crime/CounteringTerrorism.htm

[17] www.epsrc.ac.uk/ResearchFunding/Programmes/DE/default.htm

[18] http://www.epsrc.ac.uk/CMSWeb/Downloads/Calls/DEHubs.pdf

[19] "Research intelligence – when minds come together across the virtual 'sandpit'", *Times Higher Education,* 25 Sept 08

This intangible benefit is difficult to measure beyond the statements of the academics who participated in the Three-Year Review, such as:

- “One strength of the Project was the networking opportunity; I am still in touch with a number of people from the workshops I attended and I think that was valuable”;
- “the experience of working on the Project has been invaluable … [it was] extremely stimulating both in terms of the knowledge I gained and the increase in my network of contacts”; and
- “For me the process and the publications of the Project proved useful, not the least because of their inter-disciplinary quality”.

Similarly, most, if not all, of the Project experts continue to promote aspects of its findings in various academic and professional fora, both in the UK and internationally.

ii) Publications

The Project has influenced a number of publications, including:

- Mansell, Robin and Collins, Brian S. eds. Trust and Crime in Information Societies (Edward Elgar Publishing, 2005);
- Wall, David. Cybercrime: The Transformation of Crime in the Information Age (Polity Press, 2007);
- O’Hara, Kieron & Nigel Shadbolt. The Spy in the Coffee Machine (Oneworld Publications, 2008);
- Stevens, David & Kieron O'Hara. inequality.com: Power, Poverty and the Digital Divide (Oneworld Publications, 2006);
- Dutton, W. H., and Shepherd, A. ‘Trust in the Internet as an Experience Technology’. *Information, Communication and Society*, 9(4): 433-51, 2006.
- Rush, Howard, et al. *Crime online: cybercrime and illegal innovation* (NESTA, July 2009)

iii) Teaching

The Project has informed the development of a number of graduate and undergraduate university courses, including:

- The University of Glamorgan's post- and under-graduate degrees in the area of information security;
- Cranfield University’s MSc in Information Assurance.

iv) Research

The Project continues to inform research, particularly the research of the original Project participants. Examples include:

- Draft proposals for another book on technology and privacy by Dr Kieron O’Hara and Professor Nigel Shadbolt (University of Southampton);

- Partly inspiring Dr Sarvapali Ramchurn's continuing research in the area of trust in multi-agent systems (University of Southampton);
- Informing the selection of experts for the University of Brighton's Centre of Research in Innovation Management (CENTRIM) and its ongoing project on "Organised Crime and Illegal Innovation"[20], which recently published *Crime online: cybercrime and illegal innovation*, (NESTA, July 2009)[21] and cites the Project as a good example of innovation and futures thinking "in a sector in which practical forecasting on cybercrime issues rarely seems to look more than six months ahead"; and
- Professor Anne Anderson (University of Dundee) continues to lecture on the topics she explored as part of the Project to a variety of audiences, including the Institute of Ideas and several branches of the British Computer Society;

d) Professional Associations and Learned Societies

Professional associations were among the most active in disseminating and responding to the findings of the Project report.

The Information Assurance Advisory Council (IAAC), the British Computer Society (BCS), the Royal Society, the Real Time Club, and the Institute of Electrical Engineers (IEE, now the IET) held a variety of workshops, dinners, and events themed on particular issues raised by the Project (such as "*Network Surveillance"* or "*Computers and Law*")

These dissemination activities tapered off after the OYR and the influence of the Project has become more nuanced. For example, the IAAC stated that "issues from the CTCP Project are an ongoing theme in all activities", including the IAAC's focus in 2007-2008 (on Identity Assurance) and in 2008-2009 (on People Centric Information Assurance). Similarly, the BCS credited a number of Project participants (and several of the Project's issues) with guiding the BCS's 2008 work on *Responsibilities for a Safer Internet*.

A number of other professional associations have engaged with the Project and its findings, which have influenced, for example:

i) The Royal Academy of Engineering's report, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*[22] in March 2007 (the majority of the report's working group had previously worked on the Project, which was "a major influence… cited several times during discussions");
ii) The formation of the new Institute of Information Security Professionals (IISP) in 2005[23];

[20] www.nesta.org.uk/organised-crime-and-illegal-innovation/
[21] http://www.nesta.org.uk/assets/Uploads/pdf/Research-Report/cybercrime-report-NESTA.pdf
[22] www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf
[23] The CTCP Project is cited as a formative influence by an official familiar with IISP. In conjunction with Cabinet Office's Central Sponsor for Information Assurance (CSIA), IISP

iii) The Institution of Engineering and Technology[24] (IET) which "continues to champion the need for dependable systems, data security and integrity, together with IT procurement and professional standards. The [CTCP] Project outcomes continue to feature as reference points in the [IT] Sector Panel's work".

e) Business and Industry
The Project's impact on business and industry has been difficult to measure and opinion among sector contributors has ranged from frustration to admiration.

The Project achieved significant impact through two important, private sector collaborations:

i) The Cyber-Security KTN, which was developed in conjunction with the Technology Strategy Board (TSB), British Telecom (BT), and QinetiQ, among others[25]. This network has proven to be a popular and enduring legacy of the Project. A number of research activities have spun out from the network and it has informed the sector's identification, tracking, and response to issues as they arise, mutate, and fade away;

ii) The Trustguide project[26] which was set up as a joint venture between British Telecom (BT) and Hewlett Packard (HP), and part-funded by the Government Office for Science (then the Office of Science and Technology), to produce guidelines on enhancing cyber trust. Trustguide is aimed at all those researching, developing and delivering ICT.

  - "Trustguide directly builds on the outputs of the Foresight Cyber Trust and Crime Prevention project and aims to pick up where Foresight finished"[27];

  - A senior e-crime expert from the finance sector described Trustguide as "one of the most significantly underestimated pieces of work; it would be worth it if this was the only thing that [the CTCP Project] achieved";

  - Building on its previous involvement in the Project and with Trustguide, BT has "made the whole Cyber Security domain

administers the Government's Infosec Training Paths and Competencies (ITPC) certificate training programmes

[24] In 2006 the Institution of Electrical Engineers (IEE), which had engaged directly with the CTCP Project, merged with the Institution of Incorporated Engineers (IIE) to form the Institution of Engineering and Technology (IET).

[25] www.ktn.qinetiq-tim.net

[26] The 2006 final report from Trustguide is available online, www.trustguide.org.uk/publications.htm

[27] http://www.trustguide.org.uk/trustguide_flyer.pdf; Trustguide's final report, published 20 November 2006, can be found here: http://www.trustguide.org.uk/Trustguide%20-%20Final%20Report.pdf

> central to its research programme within a new (2007) research centre, the Centre for Information & Security Systems Research"[28].

Generally, it was felt that the Project might have achieved greater impact if it had been more successful in securing better private sector buy-in – particularly from the financial sector, from which Foresight was unable to secure a representative – during the Project development stages.

However, a key official from the financial sector remarked that,

> In retrospect, there is some strikingly good stuff in the Project, such as Table 3.4 (Criminal Opportunity Model). These models are still relevant… The nine Project questions (Chapter 3, Evidence Base) are very good, on risk, on criminal opportunity, on privacy, and on digital forensics

Another official from financial sector working on e-crime issues was "encouraged that cyber crime has been addressed" by Government. He was pleased by the forward-looking nature of the Project, "particularly with respect to information assurance and proof of identity issues, as the banking sector is necessarily compelled to take a much shorter term view… [and] there is less funding for longer term, general thinking of this nature in the private sector".

f) International

The international impact of the Project has been limited primarily to the participation of academics in meetings overseas:

- Dr Kieron O'Hara, a member of the Project Advisory Group, is part of a working group for the EU Commission's RISEPTIS[29] committee;

- Professor Bill Dutton, one of the Project Science Reviewers, is a member of the RISEPTIS high-level advisory body[30];

- One commentator has noted the Project's impact on the EU's five-year, 6th Framework Project FIDIS (Future of Identity in the Information Society)[31], in which "many ideas from the CTCP Project have taken root";

[28] http://labs.bt.com/cissr/

[29] RISEPTIS "is a high-level advisory body in ICT research on security and trust. It was set up as an independent group of 25 personalities from industry and academia and was announced in April 2008 by [EU] Commissioner Viviane Reding. It aims at developing a European vision on research and policy for trust and security in the future Information Society" (http://cordis.europa.eu/fp7/ict/security/riseptis_en.html).

[30] RISEPTIS: Research and Innovation for Security, Privacy and Trustworthiness in the Information Society, http://www.think-trust.eu/riseptis.html

[31] http://www.fidis.net

- FIDIS has also established a journal, *Identity in the Information Society*, which was launched recently; its editor[32], James Backhouse, was a member of the Project Advisory Group;

- One Review contributor noted that many of the Project's original participants were involved in the British Computer Society (BCS) work in 2008 on *Responsibilities for a Safer Internet*[33] - in particular, to support the work of UK delegation at the Internet Governance Forum's (IGF) annual meeting in Hyderabad in December, 2008[34].

g) Impact-limiting factors

There are a number of factors that have limited the Project's impact, although several of these factors are necessary characteristics of all Foresight projects:

- Because Foresight's project outputs are freely accessible through the internet, it can be extremely difficult to identify certain impacts nationally and internationally.

- Similarly, the diverse group of experts who participated in the Project inevitably become emissaries of the Project, the findings of which must inform, at some level, their subsequent work in the field in which they have already achieved a great deal. Consequently, they – quite reasonably – may not explicitly acknowledge the Project's influence on their later work;

- Some impacts can and should be measured, but are lost because staff turnover – particularly in the public sector – has led to a critical loss of corporate memory of engagement with the Project;

- At the time of publication (2004), Foresight Projects' dedicated follow-up activities were extremely limited; typically, a little of the in-house project team's time might be made available before assignment to its next project. This limitation left the Project to be advanced largely by the Project experts, science review leaders, and by initiatives generated during the Report's development phase;

- The Project team failed to secure the sustained engagement of the financial sector which necessarily limited the Project's potential impact;

- Several Review contributors said that had government embedded the Project findings in the heart of policy development, the acute and protracted data handling problems of 2008 may have been averted.

[32] http://www.springer.com/computer/programming/journal/12394?detailsPage=editorialBoard
[33] http://www.bcs.org/server.php?show=ConWebDoc.20326
[34] http://www.intgovforum.org/cms/index.php/component/content/article/295-event-in-mumbai

- One of the most important reasons for the Project's relatively limited impact is that the Project may have been the right project at the wrong time.

    - Several contributors to the Review observed that most of the work identifying and analysing scientific evidence for the Project took place in 2002-2003, when the ICT industry was on the cusp of a major cybercrime revolution. In effect, several have argued, the report was published a year too early and, although it generated useful thinking and important findings, the dynamics of internet crime were shifting even as it was being published;

    - At the time, attention had been focussed on the high-profile activities of hackers. By contrast, there was comparatively very little e-crime until late 2003, when phishing and malware started to appear by which time most of the Project's work was effectively complete. These threats to cyber security have remained more prominent and led to a shift from hacking of high profile sites for kudos (pleasure and notoriety) to hacking for value (of goods and services) from a vast number of potential targets; the former sought internet celebrity, the latter seek to be invisible;

    - Consequently, the Project was not well timed, although it is likely (and this point was acknowledged by the same commentators) that this misalignment could not reasonably have been anticipated by the Project team at the time;

- The problem of the Project's timing may have been exacerbated by the fact that the Project's 15-year time frame was seen by many Review contributors as overly ambitious in a rapidly evolving industry.

    - The criteria for selection of a Foresight project include a futures requirement, "looking ahead at least 10 years, in areas where the outcomes are uncertain. This typically occurs where the future direction of change is rapid, current trends are uncertain or different trends may converge"[35]. Recognising the particular challenges of and anticipating the rapid changes in the ICT sector, the Project was deliberately limited to a 15-year time frame.

    - As the Project explained in its findings, "the pace of technical, social, and business change makes it difficult to anticipate and respond effectively to new vulnerabilities… As social and technical systems become more complex and interdependent, it becomes even harder to predict how systems might fail".

[35] www.foresight.gov.uk/About/Themes/Criteria_for_selection_as_a_foresight_project.asp

- Although many observers admired the willingness to take an ambitious, long-term view, the general feeling was that even five years would have been too long a timescale.

7 Conclusions

The Project has achieved useful impact in some sectors such as the Research Councils and in academia, but less so in others, most notably within government departments (until recently) and industry. The uneven levels of impact can be attributed to the difficulty embedding the Project's key findings within the policy communities of key departments as well as the loss of corporate memory of the Project caused by the relatively high staff turnover. In addition, the Project's research may have crystallised a year too early and may have missed an important shift in the nature of cybercrime. Moreover, many of the impacts of the Project have been indirect and therefore difficult to measure

Despite these limitations, however, the Project has achieved a number of notable impacts:

- The Research Councils have credited the Project, directly or indirectly, with influencing research developments in the region of £60m, across the UK. This success is largely attributable to its key role in shaping relevant responsive mode funding applications.
- Trustguide and the Cyber Security Knowledge Transfer Network (KTN) – both of which are successful collaborations with the private sector and enduring legacies of the Project.

In addition, there have been a number of more general impacts, establishing:

- A still vibrant, inter-disciplinary network activated through the workshops and meetings that shaped the Project;
- General consensus-building by pooling existing thinking and building the scientific evidence base through the Science Review commissions;
- The effect of raising the profile among stakeholders and, by extension, society in general of the central issues raised in the report.

And finally, the Project has demonstrated remarkable resilience, illustrated by its continued relevance to ongoing concerns:

- Following "the year of data loss", many of the Project's key findings on data handling, trust, security, and others, are more relevant than ever;
- Against criticisms of too ambitious a forward view (15 years), is the praise for the Project, in a 2009 publication, as a "significant forward look in the field of cybercrime"[36];
- In response to criticisms of a lack of departmental engagement with the Project and its findings is evidence that the Project informed two Home Office initiatives[37] in 2009; and
- Finally, again in 2009, the Project was credited with influencing some £3m of research funding[38].

[36] NESTA (July 2009) *Crime online: cybercrime and illegal innovation*

[37] CTCP PROJECT influenced Home Office work on Privacy and Security (April 2009) and its "Protecting the public in a changing communications environment" consultation (July 2009)

[38] as part of the EPSRC- Global Uncertainties theme, 'Detecting Terrorist Activity', July 2009.