FORESIGHT

Cyber Trust and Crime Prevention project

Gaining Insight from Three Different Futures

OFFICE OF SCIENCE AND TECHNOLOGY

Cyber Trust and Crime Prevention: Gaining Insight from Three Different Futures

Maarten Botterman
Jonathan Cave
James P. Kahan
Neil Robinson
Rebecca Shoob
Robert Thomson
Lorenzo Valeri

29/04/2004
Prepared for the Foresight Directorate, Office of Science and Technology, United Kingdom

Preface

The Foresight project, 'Cyber Trust and Crime Prevention' set out to explore the application and implications of next-generation information technologies in areas such as identity and authenticity, surveillance, system robustness, security and information assurance, and the basis for effective interaction and trust between people and machines.

In order to achieve this aim, the project has:

- produced state-of-the-art reviews of relevant areas of science
- set out visions of the future that define a range of possible outcomes
- identified possible drivers, signposts, opportunities, threats, barriers to progress and models for decision-making
- created a network of scientists, business people and policy makers that can act on the findings to influence the future
- set out some specific key challenges and engaged all of those who can address them.

RAND Europe was asked to assist the Foresight Directorate in developing scenarios (visions of possible futures) as a basis for conducting three runs of a seminar game (one per scenario), and in running the game, involving experts and representatives from government departments, businesses and civil society. The goals of these games were to:

- develop an understanding of relationships among different actors in the system
- contribute to consistent policy planning processes rather than specific policies
- put forward adaptive, strategic long-term planning ideas.

For more information about RAND Europe activities in this project, please contact:
Maarten Botterman
RAND Europe
Newtonweg 1
2333 CP Leiden
The Netherlands
Tel: 00 31 71524 5151
Email: maarten@rand.org

Contents

Chapter 1

Introduction

In March 2003, the Foresight Directorate in the Office of Science and Technology, Department of Trade and Industry (hereafter referred to as Foresight), launched the Cyber Trust and Crime Prevention (CTCP) project to explore the implications of future information technologies for effective interaction and trust between people and machines in areas such as identity and authenticity, surveillance, system robustness, security and information assurance. The project produced state-of-the-art reviews of relevant areas of science and technology and developed visions of the future in order to understand better what policies to adopt today. Particular attention was directed to the identification of technological, societal, and individual drivers of future developments and signposts to track these developments. This was done in order that policies would be based upon the opportunities, threats and barriers in the areas of establishing cyber trust and preventing crime. Throughout its activities, Foresight CTCP has been working towards the establishment of a network of scientists, business people and policy-makers who can act on the findings of the project in order to influence the future.

In October 2003, Foresight CTCP asked RAND Europe to assist the project by 'developing scenarios and system maps to engage stakeholders in a proactive and focused way with the implications of new technologies for cyber trust and crime prevention'. This mission included requests for both methodological contributions in the form of tools not yet included in the larger CTCP project and substantive contributions in the form of the content of scenarios and their employment. In response, RAND Europe developed three scenarios based upon the identified major drivers of future developments. In addition, RAND Europe designed and conducted a seminar game to employ these scenarios. These three scenarios were used to conduct three runs of a seminar game – one for each scenario – organised by Foresight CTCP, which took place between the end of January and the middle of February 2004; each run involved a different set of participants drawn from the diverse set of stakeholders concerned with cyber trust and crime prevention. Beyond the seminar game, the scenarios have been used in other components of the overarching Foresight CTCP project.

Chapter 1 Introduction

This report documents the methodological and substantive contributions of RAND Europe to the Foresight CTCP effort. Chapter 2 begins with an overview of the orientation employed by RAND Europe to approach the construction and use of scenarios for CTCP. Then we describe how we chose which scenarios to construct and how we built them. The three scenarios are presented in Chapter 2 in abstract form; their elaborated versions as provided to the seminar game participants is provided in Annex 2. We then describe the considerations used in selecting the participants for the seminar game. The design of the game itself is described by presenting the tasks that the participants were asked to do.

Chapter 3 presents the results of the seminar game. Our underlying orientation is based upon the premise that the full value of the gaming exercise comes from the use of three runs of the game which each use a different scenario, and it is this orientation that guides how we present the results. First, we present the analysis of how participants viewed the strengths, weaknesses, opportunities and threats (SWOT) of the scenarios – orientated by issue addressed across scenarios, rather than by scenario. Then we describe how we used the hindsight arising from the SWOT analysis to transform each scenario in order to benefit from that hindsight. This, necessarily, is done separately for each scenario. Finally, we present the analysis of how six signal societal applications of information technology would fare in the (revised) scenarios, again looking across rather than within scenarios. Chapter 3 is necessarily a condensation of a rich set of deliberations by the participants.

Finally, Chapter 4 presents our strategic observations and recommendations for Foresight CTCP, both methodological, in terms of future use of the scenario and seminar gaming framework developed, and substantive in terms of technological, individual, societal and governance aspects of the information society.

Following the main body of the report, annexes present the full text of the scenarios, results of the gaming runs and additional information about the modelling underpinning the scenario design and construction.

Chapter 2

Approach and Methods

In this chapter, we describe our approach to conducting a series of experimental workshops on cyber trust and crime prevention and specify in detail how this approach was implemented.

Gaining Foresight through Virtual Future Hindsight©

'Foresight' as a concept has developed from the recognition that the future is uncertain when seen from the present. If we knew for certain how the future would unfold, it would be conceptually easy (although possibly difficult in practice) to plan for the future, in order to capitalise on the opportunities offered and to prevent or mitigate the threats. In the absence of an accurate vision of the future, planners may instead choose to construct one or more suggestive futures, and then to plan on the basis of them. Such futures may be termed 'scenarios'.

There are a number of conventional strategies for constructing scenarios, each of which has been expounded by its champions with varying, and often considerable, success.

1. **Trend analysis**. Put most simply, this strategy examines the past to ascertain how change has taken place and extrapolates the direction and degree of change into the future. This forecasting analysis produces a scenario of the future that is based upon the critical assumption that there will be no major surprises. This scenario can then be used for purposes of planning.

2. **Seeking a dream**. In contrast to trend analysis, which begins with the past, this is a back-casting strategy that begins with a desirable future and then uses the scenario to identify the steps that must be taken to achieve it. A variation on seeking a dream is 'averting a nightmare'. Here, a worst-case scenario is constructed, and the back-casting exercise concerns the steps that need to be taken in order to avoid this future.

Both trend analysis and seeking a dream use a single scenario as the foundation for planning. More recent thinking, acknowledging that future uncertainty must be incorporated into the planning process, employs multiple scenarios.

3. **Trend-break analysis**. In a variation on trend analysis, the ways in which the historical trends might change are brought explicitly into play, and for each of these possible disruptions, a separate scenario is constructed. This strategy is typically employed for planning in situations where the consequences of forecasting inaccurately are large; the result is often a conservative risk-mitigation plan to guard against departures from trends.

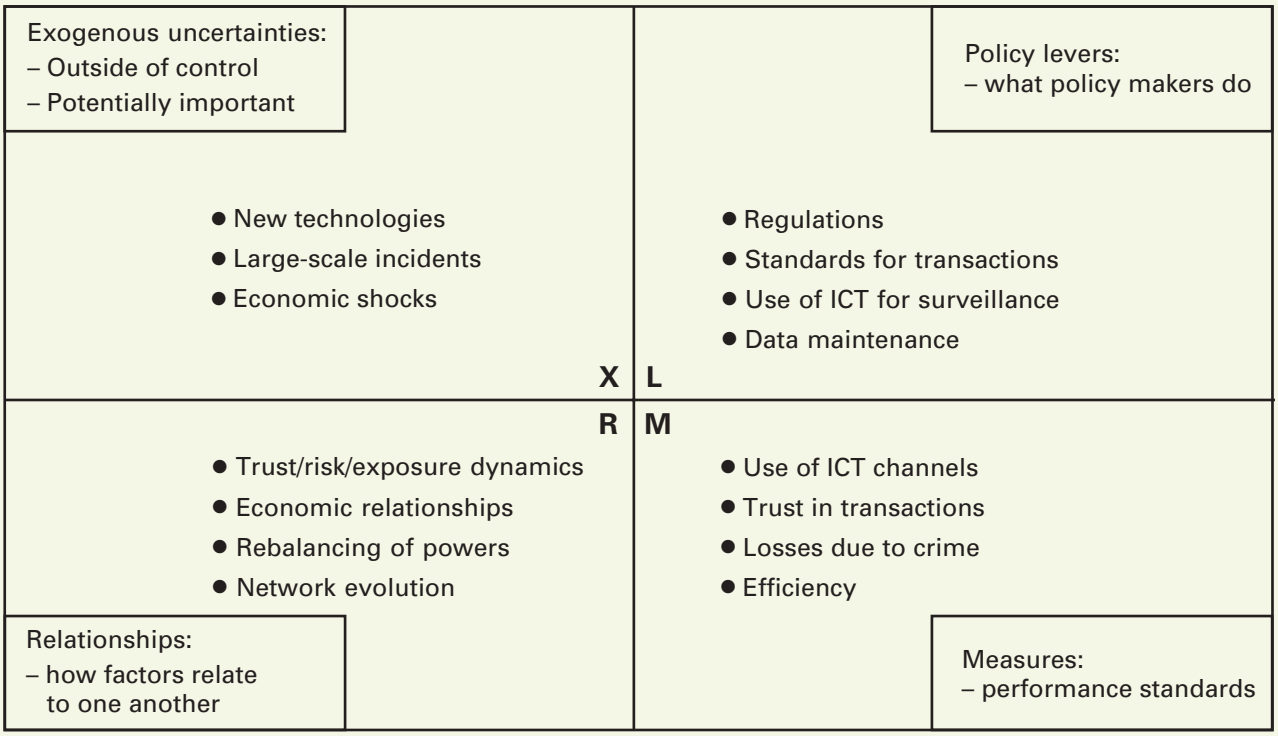
4. **Maximum expected value analysis**. This combination of trend-break analysis and the economic rational actor model designs a number of scenarios, assesses the likelihood of each, constructs measures of desirability for key characteristics of the scenarios, and plans to maximise the expected likelihood across scenarios.

Our own approach is to abandon the notion of a trend – even the most likely future is very unlikely – and to synthesise the advantages of both forecasting and back-casting strategies. The key insight is to use scenarios to disrupt the unidimensionality of time: that is, in planning for the future, we need to look forward from the present to possible futures, and backwards from the possible futures to the present. If we were in the future, we could use hindsight to see what we might have done differently to fully realise the opportunities that have been offered and to prevent or minimise the harms that have befallen us. However, we are not in the future, nor do we know exactly what it will look like. But if we imagine a number of different futures and employ hindsight for each of them, then by comparing the hindsights amongst these futures, we can identify what sort of planning is needed, regardless of which of these futures arises, and what sort of planning is dependent upon which type of future we see. This, then, is our approach to using scenarios for forecasting: to develop, in a forward-looking way, multiple scenarios based on important ways in which the future is uncertain, and then to employ Virtual Future Hindsight© to work back to present-day planning across these scenarios.

Scenarios for Gaming

This approach employs a theoretical foundation that we term the 'XLRM' Framework for understanding multiple scenarios developed recently at RAND and shown as Figure 2.1.[1]

Figure 2.1 The XLRM Framework for Scenarios



The e**X**ogenous factors affect ways in which the future is uncertain that are not under the control of the actors. Policy **L**evers are the options that are open to the various actors. There may be one or more actors who have the ability to posit policy; moreover, their separate policies may be jointly or separately implementable. **R**elationships are the ways in which exogenous factors are connected with each other and how policy will affect the world. **M**easures are ways of assessing the world, in order to ascertain, as quantitatively as possible, how desirable (or undesirable) any scenario is from the point of view of any of the actors.

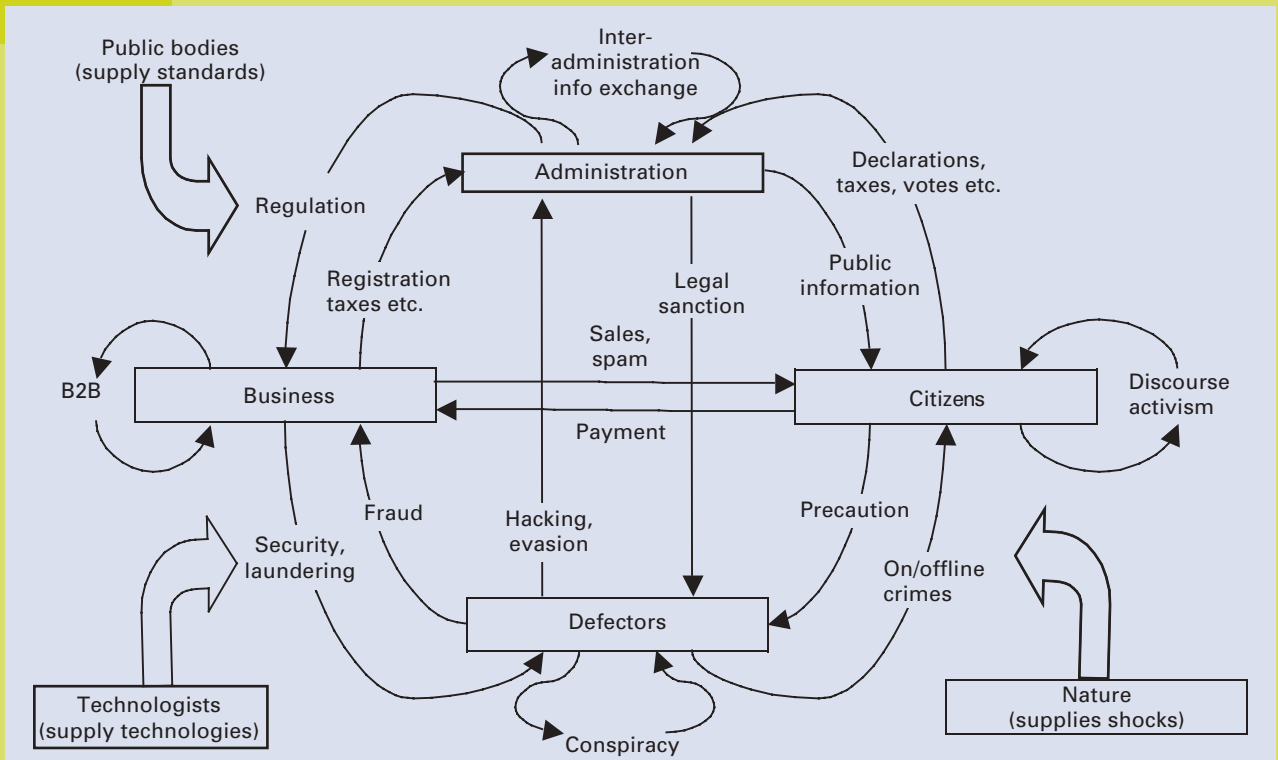
[1] Robert Lempert, Steven Popper and Steve Bankes, *Shaping the Next One Hundred Years: New Methods for Quantitative, Long-Term Policy Analysis* MR-1626-CR, 2003 available at http://www.rand.org/publications/MR/MR1626/ (visited on 25 March 2004).

The XLRM structure was developed originally for exploring very large numbers of scenarios. Many dimensions of exogenous variables are considered, which in combination can lead to literally millions of alternative futures. A computerised model is constructed that contains the relationships. Policy levers are then applied to the model to obtain values for the measures. Because of the multiplicity of dimensions and therefore scenarios, the results are displayed across dimensions to show how major policy measures behave according to variations in two or three dimensions at a time.

For this project, we adapted the XLRM structure for use in a seminar gaming exercise, where a small number of dimensions will be used to construct and flesh out a small number of scenarios based upon these dimensions. The scenarios thus combine the exogenous environment and the relationships. In the gaming exercise, participants generate their desired policy levers, as well as ways in which they measure the desirability of the scenarios that are presented to them. We also used the XLRM approach for developing the models.

The first step in constructing the modelling base for scenario construction and modification is the assembly of a listing of the salient components, combined in a generic top-level logic model of the main transactions (the main actors and the main types of transaction affected). The second step is to identify the main (XLRM) feature(s) of the scenario(s) under construction. Where relevant, these aspects may be calibrated or fleshed out by empirical data projected into the future using estimated or hypothesised relationships. The third step is to choose the main 'corners' of the scenario space – identifying the 'big idea' for each scenario, and the main implications for the elements. The final step is to construct the scenarios themselves. This involves identifying the distinguishing characteristics of the scenario and tracing through the main elements of the model to identify important aspects, the order in which they are altered, and the spill-over changes elsewhere. This process creates a 'shadow model' of impacts. The use of the models can enhance the 'concept' for the narrative, the storyboard logic of tracing effects and cross-linking and the use of numerical projections for colour and instantiation. Figure 2.2 shows the generic top-level model. More details are provided in Annex 1.

Figure 2.2 Generic Top-Level Model for CTCP



A Seminar Game for Cyber Trust and Crime Prevention

Seminar gaming is a method used to draw systematically on the expertise of a number of different people to understand a problem that contains uncertainty. It is best used in situations of mid-level uncertainty, where not enough is understood to be able to rely on formal analytical modelling tools, but enough is understood to be able to frame the problem in a logical and consistent manner. This is the situation that obtains in the area of cyber trust and crime prevention, where a common understanding of the underlying logic and the scope for intervention is most important – not least because numerical measurement is (and will remain) partial and incomplete.

Seminar games provide an opportunity to engage in semi-real decision-making without having to suffer the consequences of bad or unlucky decisions. Ideas can be explored, and chances can be taken without having to wait years to discover the results or having to fail. Moreover, in a seminar game one can have the experience of thinking things through from a perspective other than one's own. The core philosophy behind a seminar game is that by (virtually) doing, one gains understanding well beyond that which is obtainable by reading or hearing.

There are three major components to a scenario game: the scenario(s), the players and the tasking. We will present a brief conceptual overview of each component and then describe how it was implemented in the present situation.

Scenarios

For purposes of seminar gaming, a scenario is a logical and consistent picture of the future that is presented to the players. They are asked to imagine that they are actually living in the world of the scenario. It is not claimed that the scenario might actually happen (indeed, its impossibility in all of its features is often acknowledged when it is presented). It can represent a discontinuity from the present and anticipated trends. But it must be logical, internally consistent and at least plausible. Moreover, a scenario for seminar games must be concrete in enough details so that the players can actually imagine that they are in it.

Given the orientation described in the section above, we construct multiple scenarios. To do this, we identify through preliminary work the major dimensions of the future that are uncertain and make a difference. These are shown in the upper left-hand box of Figure 2.3. Aspects of the future that are important but are to be taken for granted are included in all of the scenarios, and things that do not make much of a difference are included in a creative fashion in order to provide the necessary concreteness in detail.

Figure 2.3 Elements of a scenario

	Important	Unimportant
Certain	**Include in all of the scenarios**	**Use selectively to give concrete picture**
Uncertain	**Key elements that differentiate scenarios**	**Mix 'n' match to give COLOUR to the scenarios**

The major dimensions of uncertainty are combined to create scenario skeletons. The content of these skeletons also depends on the number of scenarios to be used. The skeletons are given a suggestive name, and then fleshed out. Scenarios are prepared in both written form – typically provided in advance to the players – and in presentation form, given at the beginning of the seminar game to refresh the memories of those players who have read the written version and to familiarise those players who have only skimmed or forgotten to read the materials. In this way, at the end of the presentation, all of the players have a more or less common perception of the world in which they will be requested to live.

For the Cyber Trust and Crime Prevention Foresight exercise, we developed three scenarios set in the year 2018. The following paragraphs provide a description of the way in which we selected the three scenarios. We began by trying to map the development of information technologies over the next 20 years. Particular attention, therefore, was directed to understanding which, if any, new computing or information technology paradigms could evolve and their potential social impact. This led us to an assessment of issues such as pervasive computing, new and interdependent global infrastructures, as well as specific trends such as quantum computing and new wireless solutions.

This analysis benefited from the Cyber Trust and Crime Prevention project's *Technology Forward Look* and from the findings of several recent research efforts sponsored by the DG Information Society of the European Commission in 2002-2003.[2] These Commission-sponsored projects examined future developments in areas such as security of critical information infrastructure including:

- wireless and mobile services
- the future of electronic and physical identity
- very specific topics such as identity management, anonymity and pseudonomity.

[2] For more information about these research initiatives see http://www.cordis.lu/ist/ka2/rmapsecurity.html (visited on 13 March 2004).

We examined similar activities in the United States. In particular, we reviewed the activities of the Institute for Information Assurance Protection (I3P), a US federally funded research institution dedicated to the analysis of future cyber-security research challenges. Based at Dartmouth College, I3P brings together experts from 25 research institutions with technical, social and legal backgrounds. In January 2003, a detailed research agenda on future information security challenges was released. Particular attention was directed towards issues such as online trust, vulnerabilities, network responses, wireless, law and socioeconomic issues.[3] We also reviewed several research outputs of the US National Research Council (NRC). Through the work of several of its committees, the NRC has engaged national and international research experts to examine issues such as online authentication, the future of supercomputing, electronic records and IT support and counter-terrorism.

Our research, nevertheless, did not focus exclusively on technology. We examined the primary literature depicting trends in criminal activities and behaviours. Particular focus was also directed towards understanding the interrelationship between technology and crime policing, and the challenges of collecting and presenting evidence for crime prosecution.

In parallel to the above literature reviews, we participated in three expert workshops that were organised by the Foresight Directorate in September, October and November 2003. These workshops allowed us to better map the UK public-policy space to be examined through the scenarios. We identified, in particular, the following three dimensions of uncertainty: the balance between security and individual privacy; the dependence of society on vulnerable complex information technology systems; and, finally, the level and ownership of responsibility to counter online threats and responsibility.

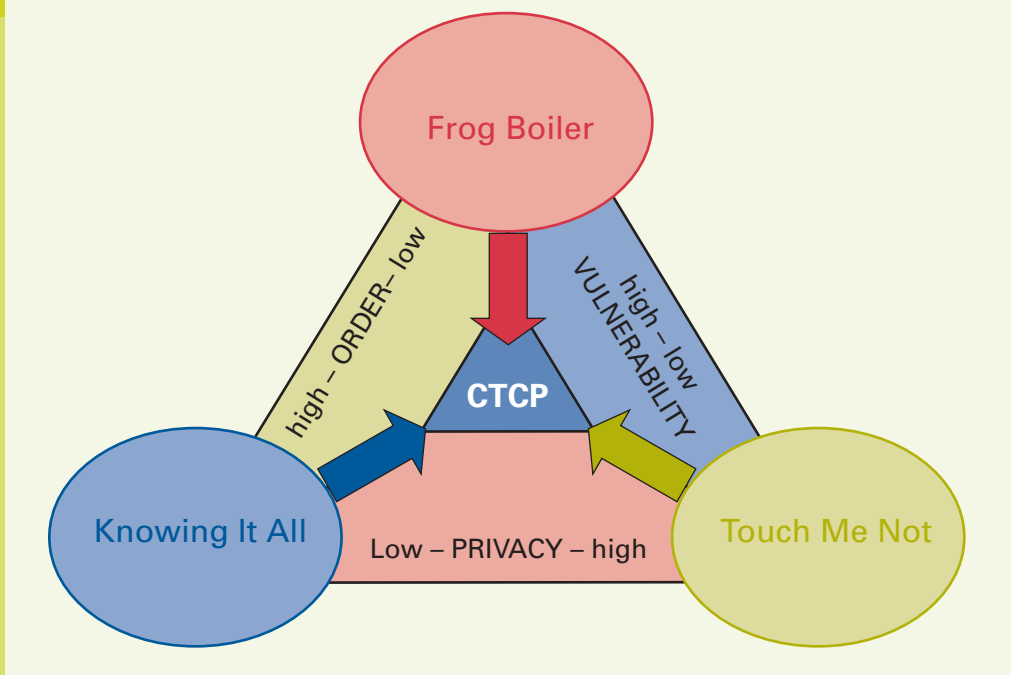
Moreover, our literature review confirmed that we were dealing with a public-policy space involving three main actors: citizens, businesses and government. Each of them has their own interests, objectives and internal dynamics. It was essential, therefore, that these elements were reflected in all three scenarios.

[3] For more information see http://www.thei3p.org/rdagenda.html (visited on 14 March 2004).

Having identified the core characteristics of the overall cyber trust and crime prevention public-policy space and its actors, we matched them with technological developments. First, we considered the same technological developments for each of the three scenarios. This allowed us to focus primarily on mapping the interrelationships between the identified actors in relation to the three identified dimensions of uncertainty of the cyber trust and crime prevention public-policy setting.

The result of this work is shown schematically in Figure 2.4. Three dimensions were considered: order, whether or not responsibility is clearly allocated for the way in which information technology is employed; the degree of privacy that exists in the world; and the degree of potential vulnerability to which people are exposed. Each scenario considered two out of the three dimensions, and left the third free to develop during the course of the seminar game. Figure 2.4 also shows the suggestive names that were given to each scenario. Each scenario is briefly described below; the full written and presentation versions are provided in Annex 2 of this document.

Figure 2.4 CTCP Scenarios



Knowing It All. In the years prior to 2018, the UK's police and intelligence services gained substantial capabilities to access and analyse information on individuals who might pose a threat to national security or who might be engaged in criminal activities. These enhanced capabilities were achieved through a combination of the consolidation of existing public sector databases, new legislation that obliged the private sector to retain and make available personal and transactional information, and new technologies that allowed this information to be used effectively. Measurable advances were made in the fight against crime on several fronts, and citizens generally approved of the concessions they had to make in terms of privacy. While the benefits of government knowing it all are widely acknowledged, there remain concerns about certain aspects of the present situation. In 2018, trust among individuals is low, and many individuals and firms believe that responsibility for security lies primarily with the state rather than themselves. While it is clear that not all vulnerabilities have been eradicated, reliable information on the nature and scale of those that do exist is missing.

Touch Me Not. Citizens are intolerant of intrusions into their privacy by government and business. Consequently, individuals are taking responsibility for security both online and offline. Cajoled by demanding and discerning customers, businesses are also taking privacy-enhancing technologies and processes seriously. In accordance with the high political salience of privacy issues, large-scale monitoring and surveillance by public authorities is severely curtailed. Vigilance and action by individual citizens and businesses have been effective in fighting certain types of crime, and the increase in individuals' acknowledgement of their responsibilities is generally applauded. However, critics point out that the emphasis on individual responsibility has exacerbated a digital divide, leaving some people more vulnerable than others. Representatives of the police and security services believe that restrictions on their powers to collate and integrate information on individuals unduly inhibit them in combating crime and terrorism. Furthermore, the large amount of private sector surveillance by individuals gives rise to the concern that privacy has been eroded, while the potential gains that could have been made by co-ordinating this surveillance have not been realised.

Frog Boiler. Information and communication technology (ICT) and wireless technologies are now an integral part of the activities of individuals, companies and public institutions. After many years of investment, the government still remains unable to provide secure electronic services to its citizens. Today, in 2018, the many faults in these government electronic systems and the management of electronic IDs and digital signatures make citizens very frustrated with these services. Some citizens even called for the re-introduction of paper-based services. Meanwhile, criminals have been increasingly exploiting government IT systems to commit fraud and cybercrime. Industry has become totally dependent on IT and wireless technologies. Investments in information security technology and management processes, however, are still limited to 2.3 per cent of the overall IT budget. These funds are not regarded as sufficient to counter the constant streams of viruses and other malicious software, as well as intrusions carried out by hackers and organised crime. It is now generally acknowledged that the police in the UK are unable to counter criminal activities involving the use of new IT and mobile technologies. In general, while people see the benefits of electronic services, they also see the associated risks.

Players

Players in a seminar game must be carefully chosen, so that they bring their own knowledge to the activity, yet do not dominate the exercise. On the one hand, in seminar games focused on policy, it is generally not a good idea to use top-level decision-makers, because they have a tendency to hold to an official position rather than explore possible futures. On the other hand, it is equally unwise to use people who know very little about the situation, because they are not likely to learn from the experience and their actions are not likely to inform the game designers. We wanted knowledgeable players who would step away from their regular professional environment, so as to achieve open and creative discussions.

Because seminar games most often examine topics where different stakeholders have different values, it is important to have people who represent various stakeholder groups (or who are at least familiar with the stakeholder positions) to participate in the game.

Players were assigned to teams and asked to take on roles. Depending on the issues involved and the objectives of the game, the roles may be natural ones (e.g. 'play yourself'), or players may be asked to take on what is termed 'cross-role play'. An example would be a department senior civil servant being asked to adopt the perspective of an information technology business middle manager. The roles assigned may be generic (e.g. 'represent the business community's interests') or specific (e.g. 'you are the senior information technology advisor to the Chancellor of the Exchequer').

The number of players in a team should be small enough to permit genuine dialogue, but large enough so that different viewpoints have a good chance of emerging. In concrete terms, this means somewhere between six and ten persons in each team. A game can involve between one and six different teams, again depending on the issues to be explored and the resources that are available to play the game.

For the series of games reported here, over 60 players were recruited from the government, business, academic and citizen communities. In the workshops they were assigned to one of three teams representing the government ('Administration team' A), the business community ('Business team' B) or citizens ('Citizen team' C). Assignment to teams was quasi-random, within the limits of distributing people as evenly as possible with due regard to the community they came from, their gender and their age. Thus, the game was one of pure role-playing rather than of natural constituencies.

Tasking

The tasking – or instruction to the players – is the core of the game. It defines the relationships among the teams and sets the agenda for the game. The players' responses to the tasking provide the data for the game analysis. The following are included in the tasking:

- how long the game will last (in time and number of sessions)
- the communication rules among the teams
- the agenda for team deliberations

- the product of the teams' labours
- how the game developers react to the players' actions and present new materials to them.

Here, we will present the tasking of each of the plays of the game by going through the two-day agenda for the session.

Figure 2.5 Agenda Structure, First Day

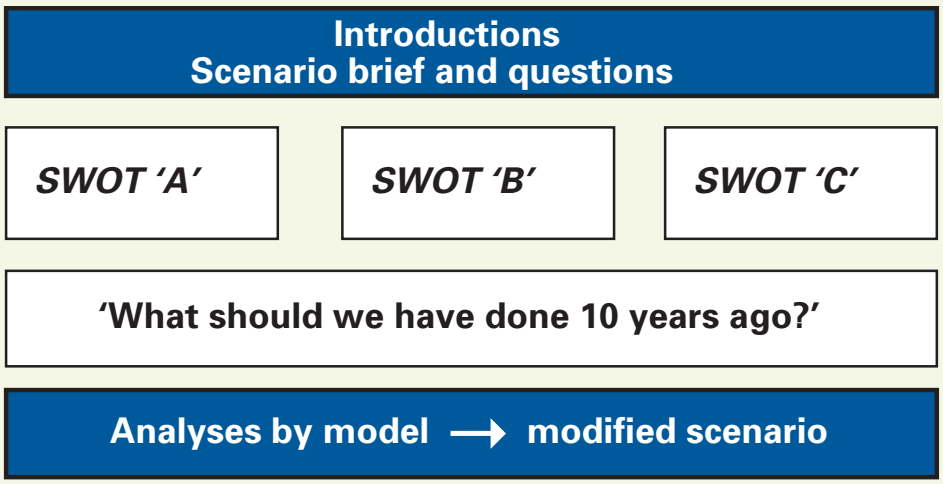


Figure 2.5 shows the agenda for the first day of activities. The game began at 13:00, after players had registered and had lunch. A general introduction was given and the procedures for the game were explained to them. They then received a presentation of one of the scenarios and were invited to pose questions about it. (In all sessions, there were only a few questions regarding the scenario.) They were then told which of the teams they had been assigned to. This first plenary session took approximately one hour.

Players then went to separate rooms, one for each of the Administration, Business and Citizen teams. In each team room, the tasking was the same, and the teams did not communicate with each other. The instructions for the teams were to complete two different tasks. The first was to undertake a SWOT analysis of the world in which they were now living. Then, taking the SWOT analysis into consideration, to think, with hindsight, about how they would have done things differently in the time period around and

shortly after 2004 in order to seize the opportunities better and mitigate the weaknesses and threats, while maintaining the strengths. This session lasted about an hour and a half.

The players then returned to the plenary, where each team presented the main points of its hindsight analysis. The separate hindsights from each team were compared, concentrating on themes that emerged in multiple teams. This session lasted approximately one hour.

The players were then released for the rest of the day. First, they heard a presentation on the wider Cyber Trust and Crime Prevention Foresight project, of which the seminar games are a part, and then adjourned for drinks and dinner. The game developers met separately and used the hindsight materials to make modifications to the scenario to incorporate as much as was reasonable, these hindsight recommendations. Thus, for each play of the game, a modified scenario was constructed.

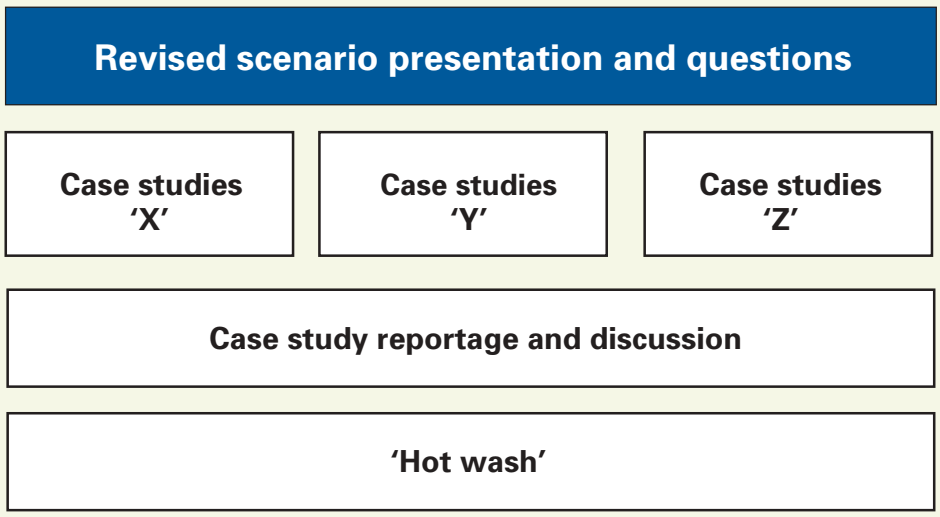
- **Knowing It All** became **Knowing What's Needed**, whereby the modified scenario incorporated rules for what data about individuals could be used and by whom

- **Touch Me Not** became **Touch Me Gently**, whereby the modified scenario incorporated elements to better guarantee trust in the use of information technologies

- **Frog Boiler** became **Leap Frog**, whereby the modified scenario incorporated procedures for measuring critical indicators of privacy, security, trust and vulnerability and institutionalised foresight activities.

Annex 3 contains the slides for the three modified scenarios.

Figure 2.6 Agenda Structure, Second Day



The second day of each game began with a 45-minute plenary session that included a presentation of the modified scenario, followed by an opportunity to ask questions about it.

The players were then presented with a description of six different broad technology application areas (referred to as "case studies" during the games) to consider in the light of the modified scenario. These case studies presented in each of the games were:

- e-payments
- online medical systems (henceforth called online medical support)
- benefits (henceforth called provision of benefits)
- customer relationship management
- forensics and evidence
- road-user charges (henceforth called road-user technologies).

The minor changes in the names of the case studies given above reflect the course of the discussions during the game, and the adjusted names will be referred to henceforth. Annex 4 contains short descriptions of the six technology application areas used in the games.

The players were then divided into new teams, arbitrarily labelled X, Y and Z. Each team had, as closely as possible, the same number of players as in the previous A, B and C teams. Team X considered online medical support and e-payments, Team Y considered provision of benefits and forensics and evidence, and Team Z considered Customer Relations Management and road-user technologies. For each case, the teams were to evaluate that case as it appeared to them in the modified scenario of 2018. Was the situation satisfactory? Was it stable, in the sense that changes were not in the immediate offing? The discussion set out to identify three lessons for the present from the analysis of the case in the future. The teams considered their two cases entirely separately from each other. This discussion session lasted about an hour and a half. (Results are given in Chapter 3.)

The next plenary session began with presentations of all of the case study lessons and a general discussion of the lessons for cyber trust and crime prevention from the entire game. The final agenda item, coincident with lunch, was a so-called 'hotwash' or critique of the exercise from the players' viewpoint. This allowed the RAND team to make improvements for the next exercise, and provide feedback to the Foresight team confirming the value of the scenarios and exercises. All three runs of the game were well received by the participants.

Chapter 3

Results of the Seminar Game

This chapter describes the main findings from the three runs of the seminar game held between the end of January and mid-February 2004. First, we report on the strengths, weakness, opportunities and threats that participants identified for each scenario. We then examine how participants would have done things differently to seize the opportunities and mitigate the weaknesses and threats, while maintaining the strengths. The last section describes the results of the participants' discussions concerning the six application areas.

SWOT Analysis of the Scenarios

The first task for the participants, undertaken in their constituency groups during the first afternoon of each run of the game, was to discuss the strengths, weaknesses, opportunities and threats of the scenario from the perspective of their assigned constituency group (Administration, Business or Citizenry). These SWOT analyses revealed a great deal of commonality in the issues that the players addressed; however, as we shall see, the way in which they dealt with those issues depended on the scenario that they were in and their constituency. Here, we present these common issues and discuss how the players approached them.

Government's Collection of Personal and Transactional Data

A major common issue was the collection and use of personal and transactional data by government. Participants in all scenarios and representing all constituencies indicated that the role of government was pivotal, as long as its processes and procedures concerning the use of data were put under independent control. If such controls were put in place, government responsibility for data collection was viewed as a strength. Still, this strength was manifested differently in each scenario.

In *Knowing It All*, participants representing Administration and Business clearly indicated that, as long as the appropriate privacy control mechanisms were put in place, increased access and

retention of data through central databases could lead to mutual benefit. Administration could use these data to understand better citizens' needs and requirements. Business also saw centralised databases as an essential repository of information to improve their quest for additional profits through more efficient and innovative marketing campaigns, products and services. Citizens could see the benefits of these centralised databases, but also the threats. Independent controls were required.

In *Touch Me Not*, the potential added value of centrally accessible databases of public information was highlighted through the weaknesses identified in this scenario. All three groups concluded that too much focus on privacy restrictions would not be beneficial. Due to limited data availability, both government and industry could not develop new services or new approaches to public safety.

In *Frog Boiler* all the constituencies indicated that the technological capabilities existed to create these centralised databases with necessary privacy controls. However, this required implementation efforts by government and business.

Digital Divide and Uneasy Society

In all three seminar games, participants concluded that future information technology developments would lead to an increased level of digital divide among individuals and an uneasy society overall.

In *Knowing It All*, there were concerns that citizens could be excluded from electronic government and commercial services if their data were not properly collected, structured and organised. In *Touch Me Not*, the strong focus on the protection of personal privacy was indirectly forcing citizens to close themselves within their private sphere with limited electronic and physical interactions with other members of society. In the case of *Frog Boiler*, all the constituencies expressed fears that citizens would retrench themselves within their personal spheres, because of the ongoing incapacity of government and industry to protect them from rising levels of online and offline criminal activities.

These fears were reinforced by the emphasis of the Administration and Business teams in all three scenarios on the threat posed by the increased difficulty of collecting and presenting evidence to prosecute cybercrimes. In both *Knowing It All* and *Frog Boiler*, this difficulty was primarily due to increased complexity in collecting and presenting digital evidence. In *Touch Me Not*, the collection of digital evidence was constrained by privacy limitations. Evidence from crime prosecution, therefore, was very fragmented and often incomplete.

Incapacity to Manage Society's Increasing Dependency on ICT and Information-Sharing

Another common finding in all three games was the strong perception among participants that society as a whole would be even more dependent on the continuing development and implementation of ICTs. In *Knowing It All*, Business and Citizens clearly identified as a threat the fact that their future activities would become increasingly dependent on government's capacity to collect and manage large databases and information infrastructures. However, the security and reliability of these databases could be easily compromised, either by technical faults or electronic attacks. This could lead to a domino effect, since Business and Citizens depended on them for their day-to-day operations.

Also, in *Frog Boiler*, the complexity involved in the management and protection of large information infrastructures by government and industry was highlighted as a major threat. A similar threat was highlighted in *Touch Me Not*. New and powerful computer and IT solutions could compromise the privacy protection of individual citizens, who would consequently be exposed to threats such as identity theft, thereby undermining their commercial and legal interactions and transactions with other entities.

The importance of interdependency was identified not only from a technological perspective. As highlighted in the analyses of *Frog Boiler* and *Touch Me Not*, the lack of communication and information-sharing capabilities among Administration, Business and, in certain cases, Citizens due to technological complexity or strict privacy regulations, was seen as both a major threat and a weakness. In the case of *Knowing It All*, the Business and Citizen groups emphasised their uneasiness at government restricting itself to data collection instead of proactively engaging in information sharing.

Trust Management

During the three seminar games, participants emphasised the increased difficulty of managing trust as a common threat and weakness. As technologies continue to grow within society, the achievement and preservation of trust are extremely complex endeavours but are also necessary to be able to benefit from the new opportunities offered by cyberspace. Nevertheless, the nature of the complexity of achieving trust varies substantially among the three seminar games. In K*nowing it All*, Business and Citizens requested that government provide evidence that their data collection and management processes would not impinge upon privacy. Government would open itself up to new opportunities in terms of enhancing efficiency through the effective use of available data, if it were able to provide evidence of independent controls over its data collection and management processes. In *Touch Me Not*, all the constituencies concluded that the major weakness of this scenario was citizens' total lack of trust in either government or business. In *Frog Boiler*, however, society's trust in new information technologies and services was constantly under pressure from rising levels of accidents, failure and online and offline criminal behaviour. In this environment, therefore, trust was not sustainable unless appropriate interventions ensuring proper use of technology were put into place.

Modified Scenarios with the Benefit of Hindsight

After they had identified the strengths, weaknesses, opportunities and threats from the perspective of their assigned constituencies (Administration, Business or Citizens), seminar participants were given a new task. They were asked to indicate what should have been done differently in the years 2004-2006. Considering the insights that they had formulated in the SWOT analyses, these hindsight observations were intended to secure the strengths, ameliorate the weaknesses and threats, and seize the opportunities inherent in each of the three scenarios. While the previous section identified some common issues that were addressed in each of the three scenarios, the way in which they were addressed differed. Therefore, we describe how each of the scenarios was modified with the benefit of these hindsight observations. Following the Virtual Future Hindsight© orientation, we treated these hindsight observations as recommendations, and will henceforth refer to them as such.

When creating the three modified scenarios of 2018 which incorporated participants' recommendations, the XLRM conceptual framework (see Figure 2.1) which informed the creation of the original scenarios was also applied. The recommendations refer primarily to the policy levers that are stated explicitly or implicitly in the scenario. The effects of these interventions work through the relationships among the exogenous factors and policy levers. The RAND Europe CTCP team met on the evening of the first day of the seminar game to elaborate the participants' recommendations in terms of policy levers, and to identify what impacts these would have. The constraints imposed by the exogenous factors specified in each of the scenarios remained the same. In other words, the modified scenarios describe the best possible worlds that can be expected, given the constraints of the exogenous factors and the benefits of participants' recommendations.

The presentation slides for each of the modified scenarios are contained in Annex 3. Here, we identify how each of the broad issues described above were addressed in the modified scenarios.

Knowing What's Needed

The *Knowing What's Needed* scenario, a modification of the original Knowing It All scenario, addressed the issues by focusing on the following main policy levers.

- An independent audit body was established as an authoritative control on government and business regarding their collection of, access to and management of information. In the original scenario, information held on individuals was seen as a strength and opportunity for improving services, yet at the same time a weakness and threat, since this could intrude upon privacy. The audit body is a policy lever that (in conjunction with other levers) allows the benefits to be obtained while protecting individuals' privacy.

- Measures were taken to educate citizens from an early age about their responsibilities regarding the protection of their personal information. This policy lever is designed to address the fact that in the original scenario, individuals left it to the state to protect their digital security. Moreover, in addition to investments in education, government and business remained engaged with individuals who were not online in order to avoid the advent of a digital divide.

- International agreements on international data transfer and data retention for law enforcement ensured that the UK did not become isolated. One of the major weaknesses and threats identified in the original scenario was the complexity of collecting digital evidence relating to crime, particularly in an international context.

By identifying and using these policy levers, the modified scenario contains outcomes that are more desirable than those described in the original scenario. These outcomes were identified by tracing the impact that these policy levers were likely to have on measures of assessment through their relationships with each other and exogenous factors. In the modified scenario, for example, a more nuanced view is widely held concerning the level of resources needed to fight crime. Given investments in education and the checks and balances imposed on government and business, resources are prioritised and targeted towards particular crimes, rather than towards the aim of knowing it all.

Touch Me Gently

The modifications applied to the original *Touch Me Not* scenario were designed to strengthen citizens' trust in government, thereby allowing government to play a stronger role in crime prevention. The following policy levers were identified and incorporated into the modified scenario.

- Political engagement with citizens and debate on the real costs of privacy. One of the main weaknesses identified in the original *Touch Me Not* scenario was the disengagement between citizens and government. Avoiding this situation requires that the choices and associated consequences concerning privacy are presented and debated by political representatives.

- Strengthened institutions to protect privacy. For example, in the *Touch Me Gently* scenario, empowered information commissioners are able to impose stronger sanctions for privacy violations.

- Education and awareness. This is necessary throughout society for two reasons in this scenario. First, given that individuals are taking more responsibility for their own security, they had better have the knowledge required to protect themselves. Second, education and awareness lead to a more informed debate about the trade-off between privacy and security.

- International agreements. As in the *Knowing It All* scenario, participants believed that the UK would be isolated internationally if the developments described in *Touch Me Not* were to take place. Consequently, international agreements, including a safe-harbour agreement and an agreement on the exchange of information, were incorporated into the revised scenario.

The use of these policy levers in the *Touch Me Gently* scenario led to more balanced decisions on the most appropriate level, whether individual or collective, at which the primary responsibility for crime prevention lies. Furthermore, by taking the lead in public debate on these issues, government has engaged with citizens with a view to winning their trust.

Leap Frog

The *Leap Frog* scenario was constructed out of the same exogenous factors present in the original *Frog Boiler* scenario, and participants' recommendations based on the hindsight provided by that original scenario. The following policy levers feature prominently in the *Leap Frog* scenario.

- Education and awareness campaigns to inform people of the real levels of the risks to which they are exposed and the actions they can take to reduce these risks. In combination with the other levers used in the *Leap Frog* scenario, this reduces the threat of individuals withdrawing from the digital world as a result of their perception of being overexposed.

- Government and business measures to promote inclusiveness. In addition to the above-mentioned educational activities that helped people take advantage of the digital world, services were also flexible, in that they catered for people who chose not to make use of the digital world, either entirely or in certain circumstances.

- Proactive planning in the form of foresight exercises and crisis management research ensured that uncertainties surrounding the digital world were gauged as accurately as possible.

- Investments in communication. These were made to improve the communication and trust among government, business and citizens. This included the organisation of a united IT security community led by the business sector which promoted a coherent strategy to reduce vulnerabilities. Secure and trusted databanks were built, containing personal data and managed by a central trusted third party. By controlling access to data, the construction of these databanks was intended to strengthen confidence. In addition, attention was devoted to ensuring the accuracy of publicly available information.

- Engaging internationally. As in the other two modified scenarios, participants pointed to the importance of this, as it would ensure that investments in the security, dependability and accuracy of information were reinforced internationally.

In the *Leap Frog* scenario, the use of these policy levers allowed government, business and citizens to engage more actively with each other. Risks associated with the use of IT were recognised and, whenever possible, ameliorated by the actions of well-informed citizens and well-designed institutions.

Case Studies

This section presents an analysis of the deliberations on six areas of application of new technologies on the morning of the second day of each session. The reader will recall that the players were divided into small groups and asked to examine two areas as they would appear in the modified scenario of 2018, and also to encapsulate their examination into approximately three lessons for each case that could be applicable to the present. The lessons are shown in Annex 5.

Methodology of Assessing Findings

Our analysis synthesises the outcomes of 18 different discussions – each of six areas for each of three (modified) scenarios. We examined the issues raised in these discussions in terms of three different relationships:

- **Robust findings** – where the discussion touched upon the same point across cases and scenarios. We operationally defined 'robust' as a point being touched upon in the same way in at least five out of the 18 discussions, including at least one from each of the three scenarios and at least three of the six areas.

- **Specific findings** – where the same point was touched upon in the same way across at least two discussions, but not enough to qualify as robust.

- **Conditional findings** – where the same point was touched upon in different ways in multiple discussions.

To this categorisation, we added a single **general finding** that was implicit in all of the discussions.

There were 18 different discussion groups, representing three different scenarios and six different applications. For ease of presentation, we have identified them by a two-letter combination, where the first letter identifies the scenario and the second letter identifies the case, as described in the following tables:

Scenario F	*Frog (Leap Frog* as derived from *Frog Boiler)*
Scenario K	*Knowing (Knowing What's Needed* from *Knowing It All)*
Scenario T	*Touch (Touch Me Gently* as derived from *Touch Me Not)*

Case B	*Provision of Benefits*
Case C	*Customer Relationship Management*
Case F	*Forensic and Evidence*
Case M	*Online Medical Support*
Case P	*E-Payments*
Case R	*Road-User Technologies*

So, for example, the acronym *KC* refers to the *Knowing What's Needed* scenario discussion on *Customer Relationship Management*, *FF* refers to the *Leap Frog* scenario deliberations on *Forensics and Evidence*, and *TP* refers to the *Touch Me Gently* findings on *E-Payments*.

General Finding

IT is not a panacea

This finding, which is in no way surprising, is noteworthy nonetheless because of the large presence of experts on information technology. It was more or less implicit and sometimes explicit in all of the discussions. This deserves mention because it derives from the way in which the entire Foresight activity has been structured. In the discussion of the ills of each of the worlds of 2018, the groups would occasionally take a step back and note that

many of the problems discussed had appeared in different guises in previous eras and more often than not would reappear in yet newer forms as technology progressed. In other words, there are some fairly constant tensions that arise from basic human social existence, and these cannot be alleviated completely by any technological solutions.

Robust Findings

Individual control is important

This point appeared in eight of the 18 lessons from the case studies, including: *FB, FC, FM, KM, KP, TC, TF* and *TM*. The point made in all of these discussions was that in order to realise fully the strengths of the (modified and more optimistic) scenario, it is important that the individuals whose information is being collected have as much control as security considerations permit over the dissemination and use of the data that refer to them. In many of the key lessons learned, a need was expressed for clear and explicit rules about who will have access to individual data and under what circumstances. The justifications governing the rules should also be open and consensually agreed across society.

Exceptions to total individual control, for security or other societal reasons, should be permitted when the benefits accrue to society rather than directly to the individual. Exceptions may be justified, for example, by early warning for threats to public safety (both malevolent and natural in origin) and the information needs of fundamental research. While different scenarios considered different mechanisms for achieving such control, and while the nature of the control issues would differ according to which case was being discussed, this central point was key to the lessons of eight of the discussions and was touched upon in many of the other ten. Thus, it deserves prominence as a key finding of the entire seminar gaming part of the project.

Supervision is necessary

This point appeared in six of the 18 discussions: *FF, KC, KF, KM, TP* and *TR*. This lesson embodies a number of suggestions about the need for close supervision in order to prevent or remediate abuses. Generally, it was believed that while most businesses and most government institutions were trustworthy in intent, there were enough potential 'bad apples' to require an authoritative supervisory

body. Moreover, even when good intent did exist, there could be bad practice requiring change. It was emphasised that the supervisory body needed to be independent; different variations of the concept provided the body with power to require access to information in order to detect and report (but not to penalise) the misuse of IT, versus a body which had enforcement and penalisation competencies. In the former instance, a prominent prototype was the National Audit Office (for UK national supervision) or international regulatory treaty bodies (for cross-national supervision).

Gain protection through multiplicity and decentralisation

This point appeared in eleven out of the 18 discussions: *FB, FK, FP, KB, KC, KF, KP, TB, TC, TF* and *TP*. The lesson was on the protective strength of diversity and a variety of paths to the same goal; if there is only one way to do something or all of the information is in one place, this creates vulnerabilities to both accidental and deliberate damage. Multiplicity was understood as 'not relying on any one system', or even one type of system for data collection, storage or transmission; having multiple systems ensured that if one system was disabled, there were parallel paths. Decentralisation referred to storage of data and information in dispersed locations, thereby providing protection in numbers. Even if one data bank was compromised, only a fraction of the information would be involved. Participants fully acknowledged that the protection of multiplicity and diversity came at a cost of some inefficiency, but judged that cost to be worthwhile.

There are trade-offs between security, trust and surveillance

This lesson appeared in six discussions: *FB, FC, FM, FP, KF* and *KP*. Although four different cases made this lesson explicit, there was no lesson from the *Touch Me Gently* scenario. Although the issues were discussed in the *Touch Me Gently* scenario groups, the privacy trade-offs central to this scenario had been addressed in the scenario modification, and therefore were less prominent in the second day's deliberations. Given this specific circumstance, we consider this a robust finding.

The lesson here refers to the need for a conscious trade-off between security and the intrusiveness of surveillance on privacy. On the one hand, one needs some surveillance in order to have security, and one needs to trust interactions. On the other hand, there is always the danger of fraud, which must be detected and

prevented. Related to this point is the question of having a single central identity versus different identities for different purposes. While there was a consensus that there was value in having multiple identities, it was also seen as necessary to know someone's identity at times, and value was seen in being able to trace somebody, under court order restrictions. This lesson is implicit in a larger dilemma that permeates the entire project: people want to profit from data availability, but are cautious about sharing their personal data.

Specific Findings

Complexity must be addressed head-on

This point appeared in only five of the discussions: *FR, KB, KR, TB* and *TR*. While these include all three scenarios, only the *Provision of Benefits and Road-User Technologies* applications had this lesson, so it is termed specific. Notwithstanding this, the issue of complexity was mentioned in other discussions but did not receive prominence. *Provision of Benefits* and *Road-User Technologies* are the two cases that were potentially regulatory in nature, so the mention of complexity for them probably reflects the prominence of complexity in contemporary debates regarding regulations.

Generally, the lessons acknowledged that IT could assist to a moderate extent in simplifying things. Due to complexity, there is a need for transparency in regulation, so as to identify and avoid unintended consequences; IT can help here by addressing the pernicious dilemma of choice between complexity and 'rough justice'. People want simplicity and transparency as well as justice that takes exceptional circumstances into account, and they want their relationships (here, largely with government) not to have unintended negative consequences.

Digital evidence is work in progress

This lesson was specific to the *Forensics* and *Evidence* case and appeared in each of the scenarios for that case (*FF, KF* and *TF*), but in no other case. In each of the scenarios, the discussion about forensics and evidence noted that there was much to be done before we fully understand how to collect and use digital evidence. Training for the police, lawyers and the judiciary was seen as necessary. This was viewed as still being a problem in any version of 2018, and therefore long-term solutions needed to be sought.

The citizen is not a customer

This lesson was specific to the *Customer Relationship Management* case, although only in the two scenarios *KC* and *TC*. In both of these groups, the lesson emerged sharply. It warns against government treating citizens as customers. In essence, it sees that government services are not commodities.

Conditional Findings

IT may affect social cohesion

This lesson appeared in two different forms. For two of the groups (FR, KR) the lesson was that IT could result in less cohesion, while in one group (FB) the lesson was that more cohesion was possible. In our judgement, both are correct. On the one hand, when the groups were worried about a reduction in cohesion, it was in the context of a potentially divisive use of technology – in this case, road-user technologies. On the other hand, when the issue was one of creating transparency and reason, IT was seen as increasing social cohesion. Interestingly, both road-user technologies and the provision of benefits can involve forms of income transfer. The case could be made that road-user technologies – which place the onus of payment on the consumers of the benefits that are provided by roads – are more equitable, and therefore might increase social cohesion. The concept of social support has been well integrated into British social thought for literally centuries, and IT is a way in which to make it less subject to the vagaries of 'rough justice'. Conversely, road-user technologies have an inherent element of over-surveillance attached, which is viewed as disruptive to society. Our overall observation is that the effects of IT introduction on cohesion are present but not always simple, and explicit consideration should be paid to them during planning.

Chapter 4

Conclusions

In this chapter we bring together the main conclusions from the seminar game for the wider Foresight effort. We frame our conclusions in terms of three themes that emerged from the workshops conducted by the DTI Foresight team prior to the RAND gaming exercise (namely technical, individual and societal) to which we add governance, a theme that arose in the gaming exercise. These conclusions need to be taken into consideration in assessing the public-policy complexities associated with cyber trust and crime prevention. Based on the issues identified, we make strategic observations and suggestions concerning the future use of scenarios, modelling and seminar games in this area.

Managing Multiplicity and Decentralisation with Technology

It is clear from the seminar games that future ICT technologies are expected to allow citizens, government and business in the UK to carry out their activities through different means and channels. Both government and business should be prepared to make their services available over a range of appropriate channels, e.g. via the Internet, interactive digital TV, mobile communications devices, post or local offices. In the case of government, the emphasis should be on finding a cost-effective mix of services – making good use of market-tested technologies and future-proofing services by emphasising interoperability and adhering to open standards.

Government and business with public service obligations should address the needs and requirements of those individuals who cannot or do not want to make use of electronic services. They should be expected and encouraged to find appropriate operational approaches to meeting their obligations. Regulations alone will not be sufficient. During several of the sessions, it was argued that ensuring access for all is key to enhancing trust and thus reducing the risk of people opting out of the digital world for inessential reasons.

Managing this multiplicity will become an increasingly complicated task in light of the expected decentralisation of ICT services and solutions. Data will be scattered across different locations around the world. More importantly, data will be exchanged constantly between various data centres. Essentially, it will become even more of a commodity on which value-added services will be built – but a commodity unlike others. Global mobile data create specific problems, including the difficulty of enforcing data protection, impediments to access to authoritative and accurate data needed to fulfil public obligations or conduct business, and possible loss of 'configuration control' – different copies of 'the same' data saying different things. These operational complexities do not only apply to industry. Government will also need to find ways and means to access and manage data for providing new electronic services and to meet its responsibilities for ensuring public safety.

Individual Control

A recurring subject concerned control over information on individual citizens or consumers. The ownership of personal and transactional data was central in each of the scenario discussions; the precise nature of the discussion depended upon the characteristics of the scenario. Empowering individuals to be able to exercise control over data referring to themselves was generally seen as a key success factor in winning individuals' trust.

Individuals' control over their personal data was particularly prominent in discussions concerning public safety. In all three scenario games, there was a general recognition that access to available data is crucial in the fight against online and offline crimes. However, it is difficult to identify a priori the data required to counter online and offline crimes. As new ICT and services develop we will see increases in the number of sensors (including CCTV, biometric access management, etc.) and in the amount of information related to transactions and traffic. The amount of available personal electronic data is potentially unlimited, and the storage of large volumes of data, as well as data mining repositories, is technically possible. In this environment data might not be in a form that could be uniquely associated with individuals or with defined owners. Therefore, negotiations about the necessary individual access to and control over data and the ability to prevent unauthorised access to those data – and the needs of law enforcement or business – will be an even more complex challenge.

Digital Divide and Social Cohesion

Digital divides and related threats to social cohesion were discussed. The single conditional finding from the study analysis is whether ICTs were an opportunity or a threat to social cohesion. This accurately reflects societal unease about these technologies. While it is recognised that new ICTs could contribute to enhancing the quality of life, many people are uncertain about how to use them and are concerned about their possible abuse.

In the absence of a concerted effort, some individuals will not have the skills to participate in, or keep up with, a more ICT-orientated society. They are at risk of becoming even more marginalised socially, and must have the opportunity to engage in society to forestall the emergence of an unmanageable digital divide. This provides added impetus to the need for extensive efforts to make literacy (including computer literacy) as universal as possible. Only a fully informed citizenry can make appropriate choices about when and how to use the expanding portfolio of ICTs that will be offered to them in the coming decades.

There will also be individuals who make a conscious decision to restrict their engagement with or to exclude themselves from the information society, even if given the opportunity to participate. This is due to the fact that they are not pleased with what they have seen and experienced. New ICTs do not always make life easier. Indeed, as the game showed, in certain cases, they can make it more complicated.

Identity theft and the misuse of personal data by individuals in industry and government will most likely not be eliminated, and people will be confronted with electronic fraud or legal errors due to 'the machine'. Because the media generally exploit the spectacular single instance rather than the quieter general trend, stories of ICT-enabled crime and heavy-handed (and misapplied) government and legal electronic surveillance and data analysis are likely to capture public attention to a disproportionate degree. This is, of course, new wine in very old bottles. Here, as the game participants often commented, there is a need for trusted information providers who can proactively inform the public, thereby countering exaggerated reports on the negative (and positive!) aspects of the information society.

Governance

To address some of the above-mentioned issues, several ideas concerning governance were put forward during the three seminar games. In each of the three scenario exercises, participants called for some form of independent, trusted third party to monitor the way in which personal data are collected, managed and used by both government and industry, in the UK and internationally. Due to the global nature of information infrastructures, the reach of such third parties should cross national boundaries.

An international response is required to counter online criminal activities that are not bound by national boundaries. Particular attention was devoted to the issue of electronic data for law enforcement and prosecution. Since data that could be relevant as evidence are increasingly to be found around the world, clear international guidelines for the collection, preservation and presentation of digital evidence are needed. However, these guidelines need to be anticipated by a clear and internationally agreed clarification of existing rules governing access to international evidence, reciprocal investigations, admissibility of foreign evidence and criminal liability for crimes committed over electronic networks from other countries (or, in the case of, for example, money laundering by satellite phone, from no country at all). To manage the threat posed by international electronic crime and to prevent the emergence of 'safe havens' for cybercriminals, this approach needs consistent worldwide implementation.

Strategic Observations

ICTs will continue to pose new challenges to benefit from opportunities and deal with risks. To manage the threats posed by new technologies, it is essential to create an environment in which government, industry and citizens can trust each other.

It will be crucial to find and maintain a generally accepted balance between the security needs of law enforcement communities and the privacy rights of individuals. Far from being incompatible in the information society, they are indispensable complements. To strike this balance, both at the national and international levels, all actors (government, business and citizens) must strive to understand and appreciate each other's rights and responsibilities. Such an understanding is a necessary condition for appropriate

implementation and monitoring. Common principles and norms need to be identified that can be transposed and implemented consistently in all judicial systems.

The scenarios and the seminar game sessions clearly indicated that technology per se will never provide the solution to foster cyber trust or to prevent crime. ICTs provide tools that need to be handled with extreme care by government, industry and citizens.

The future 'information society' requires trust. This does not mean maximum trust, since some risks are best managed by those most directly affected. It does mean that people can be provided with assurance where appropriate, and that those who bear risk understand both the risks and available means of managing or mitigating them. However, the common perception was that campaigns aimed at reminding citizens about the threats they face in an online world will not suffice. Awareness campaigns also need to highlight the potential and successes of the digital society – and *how* they were achieved.

Concluding Remarks

Over and above the strategic observations resulting from the work of the last six months, the CTCP project has also produced a tested scenario framework and gaming plan. The methodology used to build scenarios and the approach and conduct of the games have been described extensively in this document for future reference.

While the scenarios (as contained in Annex 2) have been useful for this year's exercise, it is clear that two years from now our visions of that same future will have evolved. Nevertheless, we believe that the logic and models underpinning the development of these scenarios will remain valid and useful for the rapid development of further and updated scenarios for use in similarly structured games.

We recommend repeating the CTCP scenarios and gaming exercise on a regular basis, probably every other year, to ensure continuous innovation that allows society to benefit from the new technology opportunities that cyberspace will continue to offer. This repetition should be conducted in concert with those whose actions will shape the future, and whose data-gathering and modelling activities will validate our views of the present. In this way, the validity and utility

of the scenario approach to this particular form of cross-cutting foresight activity will be enhanced. Moreover, the direct connections between the Foresight method (with its particular tools for eliciting and combining expert knowledge) and actual policy practice will be strengthened. One of the essential findings of this exercise is that successful policy needs to be based on an adaptive strategy, developed and refined by periodic – and forward-looking – re-evaluations that take into account emergent knowledge and changing objectives.

Annex 1

Underpinning Models

As mentioned in the main text, the project created a range of models to facilitate different aspects of the work. Broadly, these fall into three groups:

- System-level models of the logic underlying socioeconomic evolution of cyber trust, used to support scenario development by serving as a checklist of important components and structuring spillovers, linkages, multidimensional policy impacts and uncertainties.

- Paradigmatic or theoretical models capturing underlying cyber trust concepts, used to explore linkages and produce illustrative projections in a relatively data-free environment – since most of the underlying phenomena can only be measured indirectly (if at all) or are essentially subjective.

- Numerical models based on empirical data relating to specific transactions or infrastructures, used to calibrate scenario phenomena and initiate simple 'trend-based' extrapolations.

This annex summarises activities in relation to each of these types.

Systemic Logic Model

The scenarios themselves were primarily qualitative, as were the policy choices made by workshop participants – these choices also covered a very wide range of possibilities. It was felt that tying the exercise to a specific model would impede the working of the group and concentrate attention too much on predefined model parameters.

The overall process uses paradigmatic models to illustrate such underlying phenomena as lock-in, transmission of effects through the system, multiple equilibria and cyclic behaviour. The extrapolation model is used 'after the fact' of policy choice to calibrate the results to empirical data. The aim is not to produce predictions or quantitative assessments of policy effects (which would in any case be meaningless over such a long time-horizon

and qualitative structural shifts), but rather to calibrate the effects on a fixed number of indicators to current data and to give a sense of how their evolution is affected by scenario assumptions and policy settings.

Components

Table A1.1 gives an indicative listing of component actors, actions, arenas and measures of the scenario. The listing is too long, in that many elements will not be affected greatly by the scenario's main idea or storyline or may be at a level of detail that either obscures the scenario logic or is best left to scenario users to supply – especially when working through case studies as part of a scenario game. It is also too short; many relevant details should be supplied by scenario constructors. It is likely that the generic categories in table A1.1 and the four main actor aggregates A-D) will appear in all scenarios, however.

Table A1.1 System Components

Category	Top-level	Detailed
Elements of the system	A. Administration	Law enforcement
		Judiciary
		Taxation
		Service/benefit provision
		Information brokerage
	B. Businesses	Telecom providers (3-7 layers)
		Data-keepers
		Merchants
		Certification, etc. TTPS
	C. Citizens	Citizens
		Customers
		Community
	D. Defectors	Cyber criminals for gain
		Disruptors
		Offline criminals for gain
		Terrorists
	E. Research and technology and other NFP	Organization type (HE, PSRI, private, etc
		By domain (software, hardware, other)
		Other (standards bodies, internet governance)
	F. International	Counterparts to A-D from other countries/legal regimes
		International/multinational counterparts

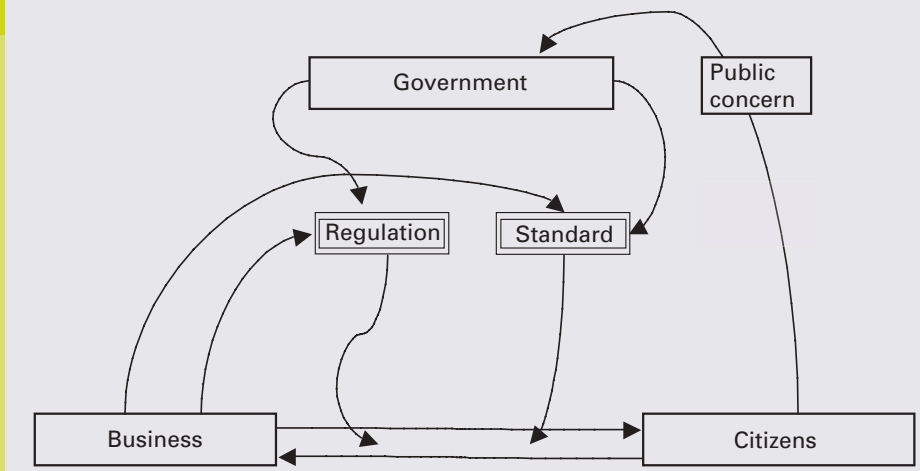
Table A1.1 System Components *(continued)*

Category	Top-level	Detailed
Types of linkage	Channels (Internet, mobile/fixed POTS, offline) – substitution/complementarity by type of transaction	
	{1-1, 1 to many, many to 1, many to many}	
	Directionality	
	Duration	
	Cost	
	Security	
Transactions	Information search, data storage, retrieval	
	E-commerce: activities (marketing, search, payment, fulfilment) and setting (B2B, B2C, A2C, B2A, C2C)	
	E-voting	
	Registration, monitoring	
	Discourse	
System properties	Network structure (clustering, diameter, connectedness, speed, reliability, etc.)	
	Resilience, sustainability, openness	
	Human, social capital	
	Norms, standards	
	Markets, political institutions, multi-party governance fora	
Objectives/ motives of agents	Profit, utility	
	Security	
	Privacy (personal information, personal space)	
	Autonomy/control	
	Uncertainty/risk	
Powers of action	Generic (apply to A-D)	Engage in transactions
		Contract
		Collect, hold, transmit, analyse data/ information
	Specific to agent type	e.g. intermediate, underwrite, escrow
	Joint/collective	
Measures of merit (quantitative/ qualitative)	Economic measures	
	Efficiency	
	Equity	
	Security	
Dynamics	Trends, trend-breaks, hysteresis, cycles, catastrophes, etc.	

Generic Top-Level Models

Figure A1.1 below shows a simplified view of the generic model in Figure 2.2 which concentrates on the issue of institutionalisation.

Figure A1.1 Main-actor logic model of cyber trust and crime



This model identifies the interaction of regulation and standards. Regulation involves specific rules concerning behaviour adhered to by actors to avoid specific sanctions imposed by a regulatory body – typically governmental – taking evidence from other actors. Standards are generic norms adhered to in exchange for participation, motivated by the benefits of, for example, interoperability. Because compliance is voluntary, it usually must be certified. Because different standards favour different parties, the process should be open. Note that in this model business has direct input into both controls, whilst citizen input comes via the government. Note also that the regulation and standards apply to transactions between businesses and citizens and not to government. This is scenario-specific.

Paradigmatic models

The paradigmatic models are developed and documented in the economic background paper. The main features used to analyse the realised trajectories of the scenarios used in the workshop were those of the 'hybrid model' – individuals have a choice between secure and insecure (hence, trusted[4]) channels influenced by, among other factors, unobserved differences in preference for the trusted channel. They learn about their environment from the experiences of those to whom they are linked (equilibrium model) or news reports and other data relating to the world at large (incomplete information/learning model). The qualitative features of the evolution are the same, but policies that change perceived risk have different impacts. The model is summarised in non-technical fashion below.

Use of the Models

The extrapolation models are used twice during the workshop. At the beginning, they are used as a data display device to generate a picture of life in 2018. After the backcasting exercise, they are used to modify the scenario:

- backcasting conclusions are used to produce time trajectories leading to the modified future
- the endpoints are used to produce the modified snapshot of 2018.

[4] It is important to clarify that an assured or certified relationship requires less trust, not more.

The paradigmatic models are used to explore the consequences of alternative assumptions and examine alternative trajectories (see graphs below).

Figure A1.2 **Extrapolated e-commerce volumes showing effect of trusted identity services**

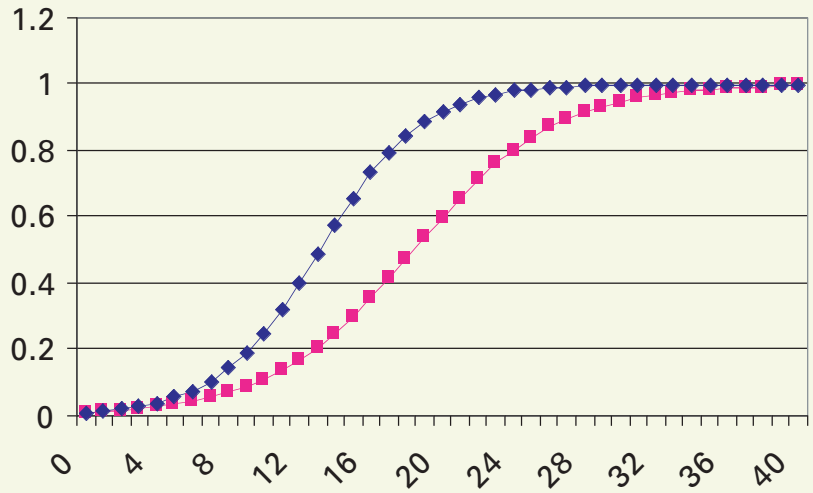


Figure A1.3 **Paradigmatic display of impact of network reach (participation) and risk (incidence of identity theft) on e-commerce, showing multiple equilibrium and hysteresis**

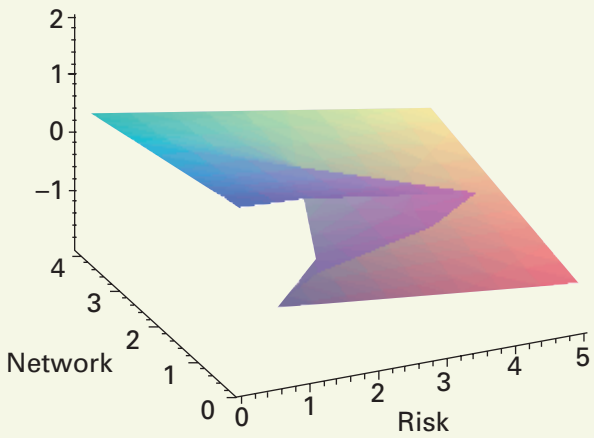
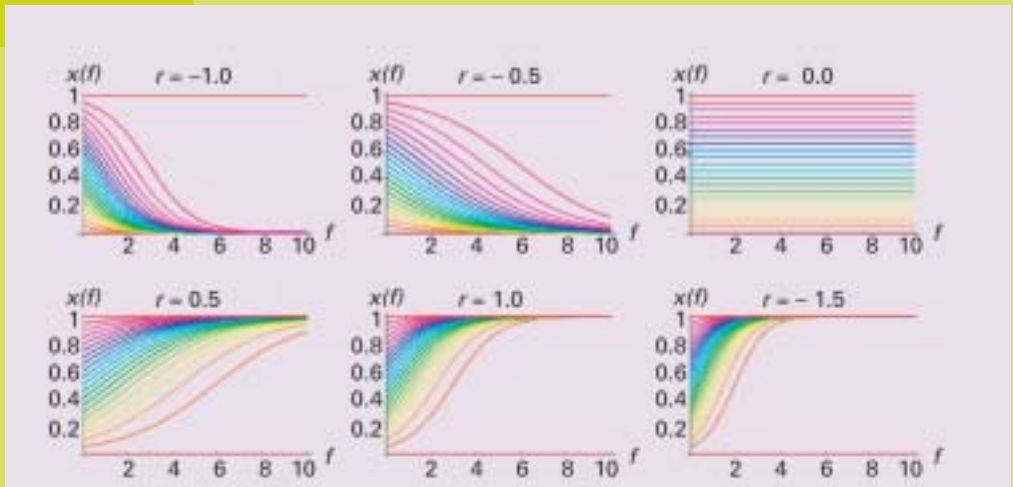


Figure A1.4 **Vensim simulation of e-commerce evolution for different 'footprints' of e-government facilities and exogenous 'risk index' (r)**



Non-technical Summary of the 'Hybrid' Model

Many trust models assume a single environment, where trusting behaviour can be analysed in terms of the differential pay-off to using a high-trust strategy (participating in a relatively insecure network). Here this approach is used to model the co-evolution of 'trusted' environment and a risky environment where individuals may behave strategically. Players have unobserved differences in the degree to which they are willing to trust the less-secure channel. To begin, we analyse equilibrium behaviour in terms of risk and exposure attributes underlying trust. This strategic model is compared to an incomplete information version in which players learn about the world indirectly via news media or summary data; the two models can be distinguished empirically.

Description of the One-sided Model

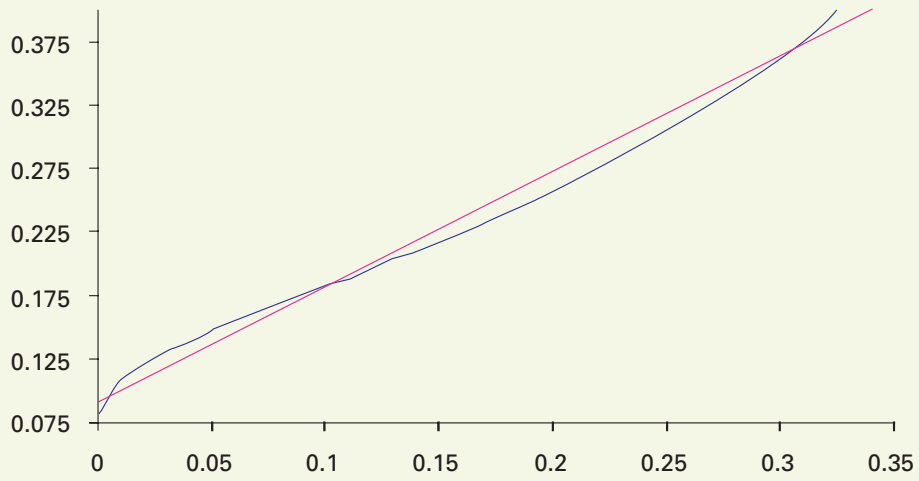
Each member of a population of linked but heterogeneous individuals can choose between a high-trust and a low-trust strategy. Players evaluate the high-trust option according to 'net benefits' minus expected 'risk cost' (which includes any costs of switching to the high-trust strategy). Net benefits are weighted by the player's

relative preference for the low-trust channel, which is not observed by others. The net benefits combine a fixed component (e.g. reduced transaction costs associated with relying on public certification) and a term that varies with the number of other high-trust individuals with whom the player interacts and the 'strength' of network externalities among players[5]. Idiosyncratic preferences are assumed to follow a unimodal (single-peaked) distribution. The next section illustrates how this set-up can give rise to multiple equilibria and how this possibility relates to the strength of network effects and the level of risk.

Equilibrium Behaviour

Nash equilibrium (rational responses to rational expectations about others' behaviour) implies that the high-trust group consists of all those whose relative taste for the high-trust strategy is 'sufficiently high' – the cut-off value rises with risk cost and falls as net benefit increases. The intersection of the two curves in Figure A1.5 shows equilibrium levels of trust for specific parameter values.

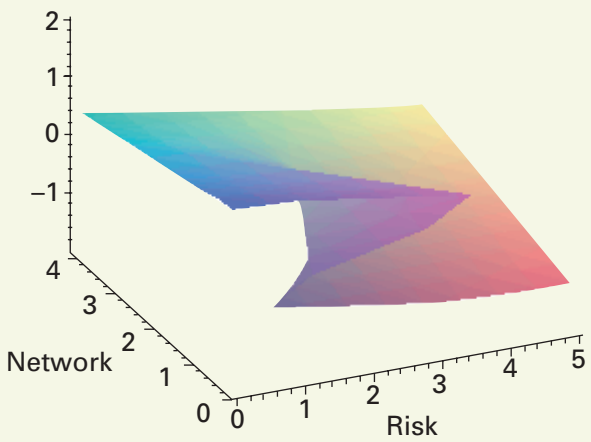
Figure A1.5 multiple solutions to the trust equilibrium



[5] The same equations arise if the risk-cost term models the likelihood of victimisation and the network-effects term models exposure.

More generally, when network effects are small there is a unique equilibrium level of trust, rising with risk cost and falling as network effects increase. When network effects are strong there are three equilibrium levels of trust (as shown above). The highest and lowest are stable and decreasing in both risk cost and network effects; the middle, unstable, solution is increasing in both parameters. Figure A1.6 shows the overall pattern, with 'trusting' measured on the vertical axis.

Figure A1.6 Equilibrium trust as a function of risk and network externalities



This illustrates the central characteristic of the model: when network effects are weak (exposure is minimal), the prevalence of trusting behaviour responds continuously and in the expected direction to changes in perceived risk. As network externalities strengthen (exposure increases), multiple solutions appear and gradually diverge.

A Two-sided Version

To complete the model, we need to consider how the underlying parameters (especially risk) respond to changes in trust, fix the strength of network effects, and assume risk responds instantaneously to the prevalence of trusting behaviour. One extreme is predation or *opportunism:* risk rises or falls according to whether trust is above or below a critical value, at which expected

returns to abuse of trust just balance expected costs (including punishment). If network effects are small enough for trust to respond continuously to risk, the model converges monotonically to the critical value and the corresponding risk level. If network effects are 'too large' the system will cycle (clockwise) in a hysteresis loop.

The polar extreme is *reassurance:* risk falls or rises as trust is above or below the critical value and the system tends towards a high- or low-trust corner solution. The same result is obtained for evolutionary dynamics in a fully connected network (except that only the high-trust corner is stable), or from a Bayesian model with partial adjustment of subjective risk estimates.

An Incomplete Information Model

Qualitatively similar results (S-shaped time paths for the creation and erosion of trust) can be obtained from a simple incomplete information model where individuals sample trust through random 'word of mouth'. The dynamics depend critically on the *credibility* of this information (whether reports of general trustworthiness are themselves trusted) and any *bias* in the reporting of relevant information (e.g. when information is selected by media or government channels to highlight negative or positive outcomes). Here, the population of high-trust individuals at any given time is a representative sample of the full distribution of tastes rather than an 'upper interval'.

Comparison

We can compare average trust per capita in the two models to see how it responds to a secular decrease in perceived risk brought about by, for example, government policy – equivalent to a fall in the critical taste parameter at which the individual is indifferent to high and low trust.

Table A1.2 Differences between direct experience and public information as sources of learning about risk

Response of trust to fall in perceived risk	Equilibrium (direct experience)	Incomplete information (public information)
No network externalities/low exposure	Fall	Constant
Peer-to-peer/high exposure	Rise, then fall	Rise

Numerical models

The basic structure linking model data to scenario workshops is shown in Table A1.3:

Table A1.3 Linkage among scenarios, cases, data, indicators and policy levers

Scenario variables	**Case study domains**	**Relevant data series**	**Indicators**	**Policy variables**
Privacy	e-Health	Identity theft	Data leakage	Identity cards
Trust	e-Payment e-Benefits e-Payments	Identity theft Viruses Incidents, vulnerabilities	Risk, exposure Expected loss	Central data repository
Digital divide	e-Benefits	Internet, mobile access by income, education	Gini	Uptake stimulation, e-government initiatives
Uptake of the Internet	e-Payments	Infrastructure, people online	Readiness	

Annex 1 Underpinning Models

Construction of the Excel-based numerical model(s) proceeded via a series of steps:

1. Data relating to infrastructure, online people, saturation, threats and vulnerabilities were combined into indicators for the scenario variables in the first column of the table

2. Dominant-relations reasoning was used to connect indicators to policies

3. Differences among scenarios were used to identify 'scenario adjustment parameters' covering both levels of data and adjustment parameters

4. Results were combined in a projection engine to translate data trends into indicator trends using:

   a) formulae from (1)

   b) trends estimated from the empirical data

   c) scenario parameters which produce step changes in levels and constant adjustments to rates of change and specifications of dynamic behaviour.

   This engine takes policy variables as inputs and produces indicator trajectories as outputs, and is implemented in Excel.

5. Trend projections are generated using one of three user-chosen alternatives (the modelling team should recommend the 'best' one):

   a) an OLS fit to a simple linear time trend (regress variable x(t) on t)

   b) a joint fit using a linear trend and one or two macroeconomic variables (e.g. consumer spending, disposable income, GDP growth rate)

   c) a 'non-linear' version using linear, quadratic and/or cubic time variables (t, t^2, t^3).

6. To move beyond simple trend extrapolation, there is an optional 'growth equation' alternative. Since data series are not long enough to discriminate among time trends, it seems appropriate to reason by analogy with other technology adoption and diffusion processes and include an S-shaped transition path. Whether a given indicator is above or below the point of inflection by 2018 depends on the scenario.

A superior alternative to a time trend with a cubic term is a logistic curve. This is the basic continuous model used to represent the evolution over time of such indicators as trust or e-commerce saturation, which have (at low levels) a network externality and (at high levels) either saturation or a congestion externality. Moreover, this specification is appropriate for nested discrete choice models and, with suitable specification choices, would allow us (given sufficient data) to take account of 'truncation at zero' in actual data. In other words, data on the use of e-commerce (for instance) tell us about the behaviour of those who use e-commerce, but not about the behaviour of those who do not – in particular, they do not indicate whether those who 'opt out' are far from the boundary of opting in. The following shows how one common form (the logistic curve) is derived.

The basic continuous time specification for an indicator I depends on two parameters:

- the maximum growth rate *r*; and
- the carrying capacity or saturation point K.

The growth equation for the indicator is:

$$dI/dt = rI(K-I)/K$$

which can be transformed by writing the indicator in relative terms ($x = I/K$) to give:

$$dx/dt = rx(1-x)$$

The solution starting from an initial value x_0 is:

$$x(t) = 1/[1+e^{-rt}\ (1-x_0)/x_0]$$

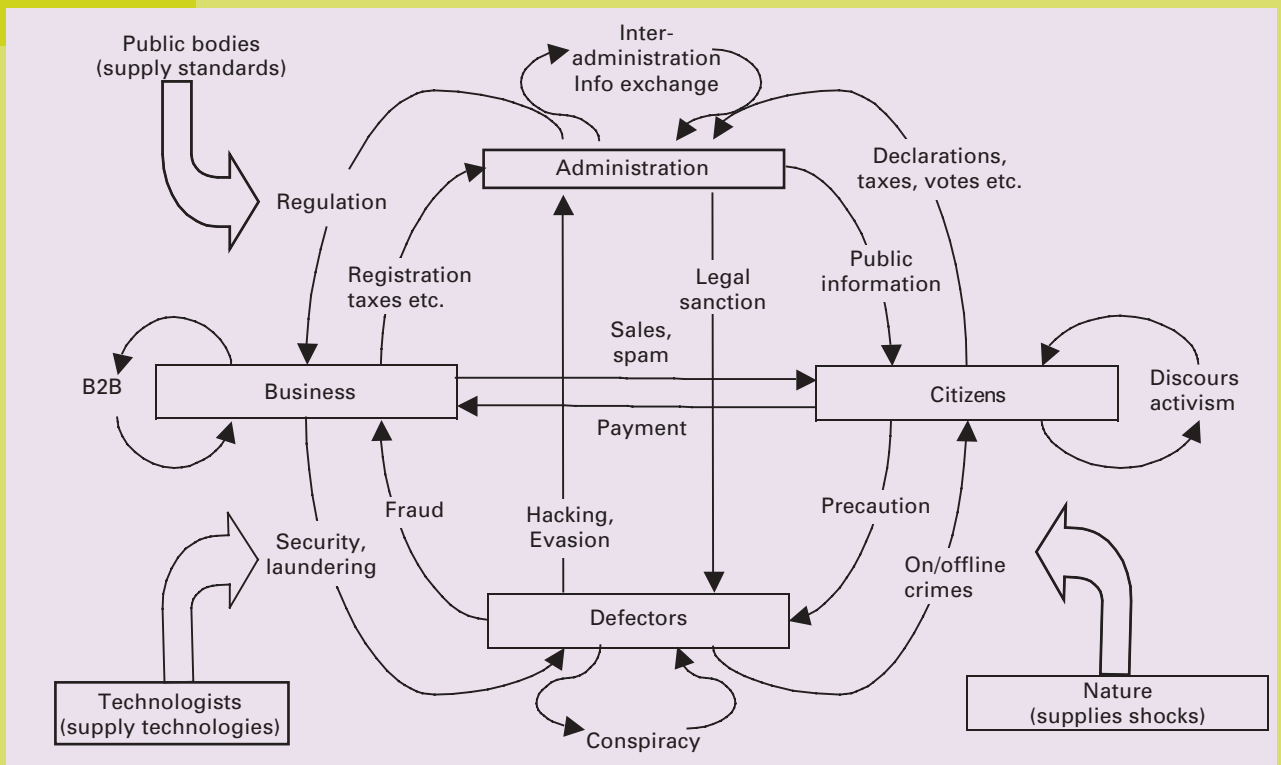
which is the logistic growth curve and shows both the desired S-shape and the possibility of multiple equilibria.

7. To link these to the scenarios, the values for r, K and x0 are derived from the data and scenario assumptions and from other indicators.

Structural Characteristics Models Implemented in Vensim

The Vensim modelling system was used to make paradigmatic projections from top-level logic models (see e.g. Figure 2.2 or Figure A1.1) using object-level representations of the major stakeholders and their transactions. The 'master version' is built around the following generalisation of Figure 2.2, as shown in Figure A1.7 below.

Figure A1.7



- *Administration* – owns regulation, enforcement, taxation and provision of some services (parts of health and education). It receives revenue from citizens and businesses and is a repository for a wide range of personal, business and public-service-related data. It is motivated by public-policy objectives.

- *Business* – owns the supply side of goods and services markets and the demand side of labour, financial and (parts of) security markets. It is the repository of commercially relevant personal information. It is motivated by profit.

- *Citizen-customers* – own online search and information behaviour, the demand side of goods and services (and part of security) markets, and the supply sides of labour and financial markets. They also pay taxes and exchange information for public services. They are motivated by risk-averse utility functions.

- *Technologists* – own variables relating to the state of technology and the rate of introduction of new possibilities in security, identity, etc. They can also own intellectual property rights (IPR). They are motivated by 'challenges' (gaps between hypothetical desired and actual levels of scientific capability, security, etc.).

- *Public bodies* – own (or take ownership of) standards and the supply side of trusted brokerage and certification services. They are motivated by Pareto Optimality.

- *Defectors* – own criminal and destructive behaviour. Their motivation is exogenous.

- *Nature* – serves as a 'black box' representation for exogenous shocks and the international mirror images of the other actors. Once the model structure is stabilised, these outside actors can be added directly.

Annex 1 Underpinning Models

Relations among the variables are driven by flows of information, goods/services, money and direction[6]. State variables are used to compute global indicators corresponding to participation, intensity of use, public and private value-added, risk probability and cost of breakdowns. These are all tracked over time to give a picture of how the situation, as measured by the empirical indicators, will change and show changes in the situation of the major actors, which in turn can shed light on their likely reaction and shifts in power.

[6] In other words, indirect control of one party's choices by another, for example, law and regulation.

Annex 2

Text of the Scenarios

Knowing It All

The Need to Take Control

The late 00's saw sustained increases in concern about crime, some increases in the levels of particular crimes, both offline and online, and several incidents of terrorism and terrorist threats. The 2007 and 2008 British Crime Surveys (BCS) revealed that over half of all respondents were of the opinion that crime at the national level had risen 'a lot' compared with the previous years.[7] In terms of offline crime, gains that had been made in previous years in certain categories of crimes were lost. The same surveys indicated steady increases in vandalism, burglaries from homes and assaults. In terms of online crimes, there were also signs that the more widespread use of new technologies had led to more opportunities for crime. Sharp increases in the numbers of identity thefts were recorded in 2007 and 2008. This was partly due to the completion of the national identity registry that revealed previously undetected cases. As the amount of data held in the private sector increased, attacks on private sector data repositories also increased. China and India became increasingly important sources of such attacks.[8] Some of these attacks were motivated by financial gain, whereby attempts were made to extort money from the victims. The scale of such attacks was unclear since victims of these crimes were unwilling to come forward. Other attacks appeared to be purely malicious. The use of 3G and 4G phones became widespread, which also created a new target for attacks, primarily of a malicious nature. While not all these crimes are solvable by imposing more surveillance, experience and media reports of them created broad support for more government control.

[7] The 2001 British Crime Survey revealed that around a quarter of respondents believed crime at the national level had risen a lot. Home Office, *'Home Office Statistical Bulletin: The 2001 British Crime Survey'*, 2001, pp. ix.

[8] Symantec, *'Symantec Internet Security Threat Report: Trends for January 1, 2003 to June 30, 2003'*, September 2003, http://www.symantec.com (visited on 19 December 2003), pp. 5. In the six months ending June 2003 China accounted for 5% of the total attack sources. The United States were the main source of attacks, with 51% of the total.

The threat of terrorism continued to dominate the agenda of international and national debates and also featured in the discussion of crime policy. Some notable achievements have been made. In 2012 a plan to disrupt a visit by the US President by a gas attack on the London Underground coupled with a distributed denial-of-service attack against emergency telecommunications systems channelled through Voice of Internet technologies were successfully thwarted. Several terrorist attacks were, however, carried out on UK and US interests abroad, particularly in the Middle East and Africa. These attacks used low-technology means – suicide bombers – to attack poorly fortified private businesses. Although the numbers of casualties were limited and the economic effects bearable, the continued presence of a terrorist threat featured prominently in political discourse. Further, the non-hierarchical, networked structure of terrorist groups made it clear that governments needed to adjust the way in which they organised their response.[9]

Persistent levels of crime, increases in concerns about crime, and the continued presence of terrorist threats created fertile ground for substantial growth in the levels of government control. In 2009, an influential Home Office report concluded that the police and intelligence services were presently unable to make effective use of the possibilities afforded by new technologies to combat crime. Increasingly, support grew for the view that the authorities should be able to make effective use of available information, irrespective of the impact on individual citizens' privacy.

Government response to crime

Government's response to these developments consisted of three main policy strands:

- improvement and consolidation of existing public sector databases
- placement of obligations on industry to retain relevant data
- phased introduction of use of new technologies in combination with enhanced information capabilities.

[9] Arquilla, John and David Ronfeldt eds. *Networks and Netwars: The Future of Terror, Crime and Militancy*, RAND, 2001.

These policy developments, which began in the early to mid 00's, were common to many countries around the world. The UK's response is therefore not out of step with international developments in the US and Europe. For instance, the US has expanded and consolidated many of its databases, both on citizens and foreign visitors. The Arrival and Departure Information System collects and registers information on visitors to the US indefinitely. Meanwhile, under the auspices of the International Airlines Traffic Agency (IATA), regional and international airlines have created a centralised passenger database through which national law enforcement agencies can check travel behaviours of individuals.

The UK Government's response began to have some positive impact by the early 10's. The success of the policy was clearly evident in increased confidence among the public in the abilities of the police services and notable reductions in several categories of crime. Victims' willingness to report crime increased and, at least for some categories of crimes, the police services were able to keep up with this increase by solving the same proportion of crimes.

Improvement and Consolidation of Existing Public Sector Databases

The completion of the identity card system was of great importance in improving and consolidating existing public sector databases.[10] A national identity register was completed by late 2005, integrating existing national insurance, tax, medical, passport, voter and driving licence records. Although introduced on a voluntary basis, the implementation of the identity card system was faster than expected since it became fundamental for carrying out day-to-day operations such as withdrawing money from cashpoints, making online payments or accessing any kind of social services. By the end of 2009, coverage was already up to 85%, a year earlier than expected. The card became compulsory in 2011, as in all other member states of the European Union. Public authorities and private

[10] Some of the events described here are based loosely on the government's identity card proposals. Secretary of State for the Home Department, *'Identity Cards: The Next Steps'*, November 2003, http://www.homeoffice.gov.uk/comrace/identitycards/ (visited on 1 December 2003). See also Department for Constitutional Affairs, *'Privacy and Data Sharing: The Way Forward for Public Services. An update on progress'*, November 2003, http://www.dca.gov.uk/majrep/datasharing/update.htm (visited on 19 December 2003); Department for Constitutional Affairs, ' Data Sharing. Privacy and Data-sharing: the way forward', http://www.dca.gov.uk/foi/sharing/index.htm (visited on 19 December 2003).

sector organisations were given various levels of access to the identity register. The incorporation of biometric identifiers – facial recognition, iris scans and fingerprints – increased the appeal of the card as a secure way of verifying identity.

Three developments contributed to widespread support for and use of the identity card and the underlying national identity register. First, during the process of creating this register, the authorities uncovered many cases of criminals using false identities. This was part of the reason for the above-mentioned increase in the numbers of identity thefts reported in 2007. Second, the system soon proved its worth in tackling identity-related crime, notably social security fraud and illegal working. Third, many businesses, particularly lenders, increasingly demanded such a card as proof of identity. These developments helped build public support for the national identity register and for more efficient use of public sector information. Some politicians argued that to a large extent this did not involve the sacrifice of more privacy; much of the information was already available to public authorities, but had simply not been integrated and put to good use before.

The national DNA database grew considerably after 2006, when police powers to take samples from suspects were expanded.[11] Increasingly, taking individuals' DNA and storing this information became seen as no more intrusive than taking and storing a photograph of them. By 2011, when the identity card became compulsory, it seemed logical to link the DNA database with the national identity register, so that individuals' records also contained DNA information. Although this is not yet compulsory, except when DNA profiles are obtained using the police force's statutory powers, citizens are free to volunteer this information. Many see this as part of their civic duty, since it can assist the police in eliminating potential suspects from investigations. As with the original national identity register, this expanded DNA database is proving to be a valuable resource in the fight against crime.

[11] The Criminal Justice Bill extends police powers to take and retain DNA samples from arrested suspects. Home Office, *'Delivering Justice for All – Criminal Justice Bill Receives Royal Assent'*, REf, CJS 010/2003, 21 November 2003, http://www.homeoffice.gov.uk/pageprint.asp?item_id=688

Placement of Obligations on Business to Retain Relevant Data

Government has clearly opted to impose a data-retention policy on business, rather than the lighter data-preservation approach.[12] Businesses that collect large amounts of personal and transactional information are obliged to retain this information. These data must be provided to the public authorities upon request. Although some public funds are provided to compensate businesses for the costs of storing and making available these data, these do not cover the full costs. Essentially, the retention of information is part of the conditions that have to be met before companies in many sectors are licensed to operate. In order to preserve the immediacy of data access, companies that outsource their IT operations or extensively use web services through foreign countries are expected to request an appropriate government licence with strict technical and human resources requirements.

Some of the data that businesses are required to retain and pass on to public authorities on request include the following:[13]

- Communication service providers are obliged to store pre-identified types of data covering a broad range of transactions and communications for a period of ten years. These include mobile phone geopositional locations, Internet chat-room dialogues, e-mails, postal forms and phone call records.

- Travel companies must store a wide range of information for the same ten-year period, including air travel itineraries, parking times at airports, car rentals, hotel reservations, road tolls and train itineraries.

- Financial services providers are obliged to retain information including their customers' credit card applications and transaction reports, loans and all financial transactions.

[12] ICC, UNICE, EICTA, INTUG, *'Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes'*, 4 June 2003, http://www.iccwbo.org/home/news_archives/2003/stories/data.asp (visited on 1 December 2003).

[13] Most of the following examples were taken from an extensive list provided by Jonas, Jeff, *'Appendix H: The Landscape of Available Data'*, in: Merkle Foundation Task Force on National Security in the Information Age, *Creating a Trusted Network for Homeland Security,* 2 December 2003, http://www.markletaskforce.org/ (visited on 4 December 2003).

Of course, much of this information was collected before the adoption of the new data-retention laws. However, government intervention was required to ensure that this was done consistently, over a sufficiently lengthy period of time, and in a form that provides useful intelligence.

Gradual Introduction of New Technologies

New technology has been introduced gradually, taking advantage of existing infrastructures. Widespread use of biometric technologies for identification purposes was slower to take off than some policy-makers had anticipated in the early 00's. Until the mid 10's such identifiers were used almost exclusively for the purposes of identity verification. Despite encouraging experiments with facial recognition in some local authorities and high streets[14], it was not until the mid 10's that this technology matured. Nevertheless, the incorporation of facial recognition identifiers in the national identity register and the digitisation of CCTV services meant that when the technology did mature, the information infrastructure enabled the police services to make full use of it. CCTVs now offer almost seamless surveillance in most urban areas.[15] Furthermore, the widespread use of biometric technology for verification purposes prepared the public for its use in identification.

A complete facial recognition system is currently being rolled out across all crime hot spots.[16] It links the existing CCTV installations with the national identity register containing facial identifiers, with further links to lists of suspects or individuals wanted for questioning. Video streams are sent over a network to a regional control room. In the central facility, state-of-the-art facial recognition technology identifies faces in these video streams and matches

[14] A report of the US General Accounting Office questioned the use of facial recognition technologies for identification purposes. GAO, United States General Accounting Office, *'Technology Assessment: Using Biometrics for Border Security'*, November 14 2002, http://www.gao.gov/ (visited on 1 December 2003). See also the results of the Face Recognition Vendor Test, http://www.frvt.org/FRVT2002/default.htm (visited on 9 December 2003).

[15] The Independent, 'Big Brother Britain', 12 January 2004, http://news.independent.co.uk/uk/this_britain/story.jsp?story=480364 (visited on 12 January 2004) reports that in Britain the number of CCTV cameras quadrupled between 2001 and 2003; in 2003 there were four million CCTV cameras in the UK (a fifth of the world's total), making Britain one of the most watched nations in the world.

[16] For a model of a facial recognition surveillance system see Woodward, John D. Jr., Christopher Horn, Julius Gatune and Aryn Thomas, *'Biometrics: A Look at Facial Recognition'*, *Annotated Briefing*, RAND, 2003.

these with a database of target individuals. Trained officers then check the probable matches to ensure false alarms are identified and recorded. If the match is confirmed by the officer, local police are then informed of the individual's whereabouts.

Delivering Results

The above-mentioned expansion of databases containing personal information, increases in police powers to access and analyse these data, and the roll-out of new technologies led to measurable advances in the fight against certain crimes and in public confidence in the police services. The increase in the numbers of certain criminal activities reported up to 2012 followed by a levelling off is believed to be the result of three developments. First, there was a real increase in the numbers of crimes perpetrated. Second, some crimes, in particular identity thefts, became more readily detected with the construction of the national identity register. Third, individuals became more inclined to report crimes since they gained confidence in the police force's ability to solve them. The British Crime Survey revealed an increase in the percentage of crimes reported from 45% in 2000 to 65% in 2015. Despite the large increase in the numbers of crimes reported, the percentages of reported crimes solved remained relatively constant for several important categories.

With this success came increased demands on the law enforcement services. New technology has helped somewhat in streamlining administrative processes. However, it has become clear that effective policing is impossible if strict lines of demarcation are imposed between actors who can potentially contribute to the fight against crime.[17] Instead, the effectiveness of the system has been strengthened by an increasingly inclusive security community. This includes all local-level government officials who may encounter useful information: for example, local police on the beat, airport officials, social workers and staff in hospital emergency wards. The security community encompasses not only the police force, which has expanded steadily in recent years to

[17] Merkle Foundation Task Force on National Security in the Information Age, *Protecting America's Freedom in the Information Age*, 7 October 2002, http://www.markletaskforce.org/ (visited on 4 December 2003); Merkle Foundation Task Force on National Security in the Information Age, *Creating a Trusted Network for Homeland Security*, 2 December 2003, (http://www.markletaskforce.org/ (visited on 4 December 2003).

250,000 police officers[18], but also approximately 300,000 individuals working in transport services and social and health services. Following the Parliamentary approval of the new Private Security Industry Bill, members of the security community are authorised to record information they deem relevant in the system, making this available to police services. Although government guidelines limit the access ordinary citizens have to public records to protect privacy, the ability to pool information from various sources has helped solve many crimes that may otherwise have not been solved.

The success of the Government's response to crime can also be seen in the increasing demands on the judicial and prison services. New technology helped somewhat in streamlining administrative processes. The ability of the courts to cope with the enormous case load was improved by the more widespread use of trial by judge; trial by jury is nowadays reserved for serious offences. The prison population in England and Wales rose to 130,000 in 2017, compared with 100,000 in 2009 and 65,000 in 2001, 80% of which is now hosted in privately run companies.[19] Over the past ten years a broad political consensus has supported increased spending on all aspects of law and order.

Patchy Business Response to Crime

The main policy developments described above in response to crime were led primarily by government. Business and civil society were rarely consulted. The essentially one-way information flow from business to government did not provide businesses with the information required to make accurate risk assessments. Moreover, the government-led response did not engender a sense of urgency in business that action was necessary, nor did it instil any notion that it was the responsibility of business to take the lead in this area. Therefore, the private sector has been reluctant to make investments in securing the large repositories of information they hold. Some had forecasted that users would demand and be willing

[18] Back in August 2003 there were 136,366 police officers. Home Office, *'Home Office Targets Autumn Performance Report 2003'*, Cm 6057, December 2003, http://www.official-documents.co.uk/document/cm60/6057/6057.htm (visited on 6 January 2004).

[19] Councell, Rachel and John Simes, *'Projections of Long Term Trends in the Prison Population to 2009, England and Wales'*, National Statistics, 9 December 2002, http://www.homeoffice.gov.uk/rds/pdfs2/hosb1402.pdf (visited on 9 December 2003). In one scenario, these authors project a prison population in England and Wales of 109,600 in 2009 compared with 65,000 in 2001.

to pay for high levels of security as the amount of retained data grew. With the exception of a few elite market segments, this demand has not materialised. This has led to a patchy distribution of security measures. Only a few companies are legally obliged to invest in security measures. For example, broadband Internet providers were obligated to provide virus-protection software after several damaging worm attacks on insufficiently protected 'always on' connections. They are also expected to provide content filtering mechanisms that both protect individuals from online illegal content and automatically update a centralised government database. In this context, the Government also provides the necessary keywords to screen the content, although certain individuals are excluded from content monitoring since access to certain content, such as medical information, is necessary for their professional activities. However, this exclusion needs to be granted through an ad hoc licence issued by the central government. Specific agencies monitor the behaviours and the licence is withdrawn immediately if unjustified violations are detected.

Business models that make use of the large repositories of information held in the private sector have matured. In order to assist companies in complying with government requests, there has been a considerable growth in private sector services that systematise the records held on individuals and businesses, providing companies with credible information on the activities of individuals and companies with whom they transact.[20] The use of background searches using these services is now commonplace. Such services have allowed companies to recuperate some of the costs incurred by the mandatory preservation of large amounts of information. The limited access such services have to information held by public authorities is criticised by transparency advocates who argue that the only way to secure freedom in a society with pervasive surveillance is for powers of observation and surveillance to be shared by all.[21] Transparency advocates have largely replaced privacy advocates in providing criticism of government control and use of information.

[20] An example of such a development is the Global Regulatory Information Database (GRID) operated by Regulatory DataCorp, Int. LLC (RDC), http://www.regulatorydatacorp.com/ourServices.html#grid (visited on 5 December 2003). GRID contains approximately 1.5 million individual and business names drawn from over 22,000 international and US public record sources including government lists, media and regulatory actions.

[21] David Brin, *The Transparent Society: Will Technology Force us to Choose between Privacy and Freedom?* Reading MA, Perseus Books, 1998.

Individuals' Response

The lack of user demand for security has been attributed to users' confidence in government to take the necessary steps to protect their interests. Legal obligations on communication service providers, such as compulsory virus protection and content control, have not encouraged consumers to be discerning regarding security when it comes to selecting alternative services and products. Indeed, consumers appear to hold the view that government has taken the necessary steps to ensure the online environment is secure, and that they need not concern themselves with this.

Most people are bewildered by small number of protesters and activists who worry about the current situation. They seem to be arguing either that there is too much government intervention, in the form of snooping, or that government should intervene more by taking control over large databases of personal information. Only few, usually well-resourced, individuals and businesses invest in privacy and security-enhancing technologies that enable them to conduct their activities in secret. At best, this is viewed as somewhat freakish, and paranoid to a point that UK research councils have stopped funding academic activities in this area. More commonly, the use of privacy-enhancing technologies is viewed with some suspicion; these individuals obviously have something, probably illegal or immoral, to hide.

The Benefits of Knowing It All

Policy-makers point out that the increases in government powers have increased the effectiveness of the fight against crimes on several fronts. The identification of perpetrators of offline crime, particularly shoplifting and street crimes, has become much easier. Certain types of online crime, notably online identity theft, have been all but eradicated. Public confidence in the police services has increased. Granted, this does not mean that the public feels safer. Fear of crime seems to have stabilised around the high levels recorded in 2010.

Aside from the benefits in terms of crime prevention and detection, the ability to verify the identity of individuals and businesspeople has had enormous positive effects on online commerce. For instance, individuals now conduct most mundane shopping online and physical stores are reserved for fun shopping. Niche markets have also developed which consist of of the small minority of consumers that refuse to take advantage of the convenience offered online.

Considerable savings have been made in the public sector.[22] The national identity register soon replaced separate systems for national insurance, tax, medical, passport, voter and driving licence records. Total public expenditures have, however, remained stable, since the savings were passed on to the police and prison services. Expenditures on law and order have risen from approximately 6 per cent of public expenditure in 2002-2003[23] to 15 per cent in 2017-2018, the same level of priority given to expenditure on education.

The national identity register also laid the foundations for more intensive forms of online civic participation.[24] Large-scale experiments with e-voting were held successfully, although this did not lead to the much-hoped-for increase in turnout. Many see the current technologies and increasing blurring of the boundaries between the online and offline worlds as fertile ground for more participatory forms of democracy, based on plebiscites on specific issues.

Concerns Regarding the Future of Knowing It All

Despite the successes booked by the police services in the recent past and hoped for in the future, there are concerns regarding the effectiveness, economic costs and legitimacy associated with the current response to crime.

As the sheer volume of data retained by business and government increases, critics question the usefulness of this information for detecting and solving crimes. Although advances in data-mining techniques have allowed relevant data to be gleaned from larger databases, there are signs that the volume of data is becoming unmanageable.[25] Some warn that criminals and terrorists may be

[22] The benefits of IST to the provision of government services is discussed in Botterman, M. et al., *'Moving towards a Knowledge Society: the IST contribution to eGovernance'*, JANUS, Joint Analytical Network for Using Socio-economic Research, May 2003, http://www.janus-eu.org (visited on 1 December 2003).

[23] Emmerson, Carl, Christine Frayne and Sarah Love, *'A Survey of Public Spending in the UK'*, December 2003, The Institute for Fiscal Studies, Briefing Note No. 43, http://www.ifs.org.uk/public/bn43.pdf (visited on 12 January 2003).

[24] Papandreou, George A. ed., *'Special Issue: on e-Democracy', The Institute for Prospective Technology Studies Report,* vol. 75, (June, 2003).

[25] The UK government's current plans for an ID card have been criticised on similar grounds by Privacy International: Statewatch, *'Statement by Privacy International concerning the Government's proposed National ID Card',* 11 November 2003, http://www.statewatch.org/news/2003/nov/05ukid.htm (visited on 24 November 2003).

able to disappear in this mountain of data. In addition, as mentioned above, the existence of poorly fortified data repositories in some parts of the private sector creates new vulnerabilities that may be exploited by criminal individuals or organisations.

Although businesses have been able to recuperate some of the costs of retaining data by selling this to information agents who consolidate and sell this data on to others, compulsory data retention is nevertheless a burden on the economy. The costs vary considerably by the type of industry concerned. Such costs have long been, and continue to be, high in the financial services sector where substantial resources have to be set aside for monitoring transactions.[26]

Concerns have also been raised regarding the legitimacy of the current response to crimes. It is estimated that there are around 50 false-positive incidents each year, whereby innocent individuals are apprehended, usually on the basis of information collected by CCTVs linked up with the new facial recognition technology. The authorities assure the public that all are detected before any serious consequences occur. The current debate focuses on whether this is simply the price that has to be paid for security. In addition, some worry that proof of a serious false-positive incident could undermine public support for the resources made available to the security community. The security community is also concerned about the information disseminated by civil liberties campaigners. Although such groups play an important role in getting the balance of state power right in an open society, they need to be monitored closely to ensure that the information they disseminate is accurate. In the face of the persistent threat of terrorism, many public figures are calling for a consolidation of the gains that have been made. For some, this means more intensive forms of international co-operation and data-sharing.

Some people have voiced the concern that the UK has become locked into a downward spiral in which a lack of trust among

[26] Some of the measures required for the effective combat of criminal and terrorist money laundering and financing are outlined in the following sources: OECD, Financial Action Task Force on Money Laundering, '*The Forty Recommendations*', 20 June 2003, http://www1.oecd.org/fatf/pdf/40Recs-2003_en.pdf (visited on 18 December 2003); GAO, United States General Accounting Office, *'Terrorist Financing: US Agencies Should Systematically Assess Terrorists' Use of Alternative Financing Mechanisms'*, November 2003, http://www.gao.gov/new.items/d04163.pdf (visited on 18 December 2003).

individuals feeds and is in turn reinforced by the demand for increased levels of surveillance[27]. Individuals appear to have developed more confidence in some public services – in particular policing, evident in the increasing percentages of crimes reported. At the same time, their trust in generalised 'others' has fallen to all-time lows. In 1999, 30 per cent of British respondents agreed with the statement that 'generally speaking, most people can be trusted'[28]. This figure is presently 10 per cent. Some blame the prevalence of widespread surveillance for this decline in social capital. They argue that this lack of trust among individuals strengthens the demand for information on and surveillance of others, which in turn erodes trust further.

Touch Me Not

Individuals Taking Responsibility

Britons are fiercely protective of their privacy. Members of the public are taking responsibility for protecting information about themselves, and their privacy demands have been communicated effectively to government and businesses. Issues concerning the protection of information on individuals as citizens and consumers are now at the top of the agendas of public and private sector decision-makers. The most important priority is to ensure strict adherence to the rules concerning the storage of and access to personal data. In contrast to the United States, UK law enforcement services have not been given access to vast public and private sector databases containing information on individuals and companies. There are strong legal safeguards ensuring that individuals have full control of the use of personal information by government bodies and companies. Government and business responses have included the introduction of privacy-enhancing technologies and processes that improve the security of their information systems. The main reasons for the increase in the level of priority given to privacy were:

[27] This possibility was raised at the Foresight Cyber Trust and Crime Prevention workshop, '*The Societal Impact of S&T: Risk and Trust*', 6-7 November 2003.

[28] The third wave of the European Values Study held in 1999 contained the question 'Generally speaking, would you say that most people can be trusted or that you can't be too careful in dealing with people?'. 29.8% of British respondents said that most people could be trusted. Of the countries surveyed, the lowest percentage of people who said that most people could be trusted was Romania with 10.1%. Halman, Loek, *The European Values Study: A Third Wave*. (Tilburg: EVS, WORC, Tilburg University, 2001).

- fears relating to the creation and linkage of large public sector databases containing information on citizens. It was feared that this would lead to unwarranted intrusions into personal life. Further, many believed that government bodies would be unable to build and use such information resources accurately and effectively

- intolerance of increasing levels of online nuisance. These forms of nuisance ranged from spam marketing on e-mail and new-generation mobile phones to malicious online attacks that targeted individuals and businesses. Increasingly, individuals realised they could not rely on service providers to protect them from such intrusions; they had to take action themselves

- resentment at the increasing lack of privacy in the offline world. For instance, following technological advances, camera surveillance became even more ubiquitous in the mid-to late 00's. Members of the public became increasingly aware of the fact that their whereabouts and activities were being monitored by public and/or private sector organisations.

Technologies and practices that facilitate privacy protection and security have, moreover, advanced to a stage that they are affordable for, and can be used easily by, a large proportion of the public. Companies have responded to the growing market for these technologies. Improvements in cryptographic technologies and processes make it cost-effective for privacy technologies to be deployed in everyday communications and in many devices.[29] Most people nowadays block communications that are not encrypted. Privacy-enhancing technologies and procedures allow individuals to reliably protect their communications from unwanted intrusions, to verify the identity of the parties involved in the communication and to guarantee anonymity when desired. The use of agents and anonymous e-money allows individuals to transact without revealing their identity. Purchases via agents are accepted by most online retailers, even for small everyday transactions.[30]

[29] Lin, Guo-Shiang, Hsuan T. Chang, Wen-Nung Lie and Cheng-Hung Chuang, '*Public-key based optical image cryptosystem based on data embedding techniques*', Optical Engineering, Vol 42, Issue 8, 2331-2339 (August, 2003). Uchida, A., P. Davis, and S. Itaya, '*Generation of information theoretic secure keys using a chaotic semiconductor laser*', Applied Physics Letters, Volume 83, Issue 15, pp. 3213-3215, (October 13, 2003).

[30] Shari Trewin, '*Configuration Agents, Control and Privacy*' in Proceedings on the ACM 2000 Conference on Universal Usability, pp.9-16.

The public's concern with privacy in the online world is accompanied by a heightened state of alert and willingness to take personal responsibility for security in the offline world too. One explanation for this is that the law enforcement services' ability to fight crime is currently far below its potential, and individuals are responding to this rationally by taking more responsibility. In 2011, an influential Home Office report concluded that the law enforcement services were presently unable to make effective use of the possibilities afforded by new technologies and data sources to combat crime, both offline and online. One of the main reasons cited for this inability was the tight legal restrictions on sharing and accessing information contained in both public and private sector databases. Another explanation for increased personal responsibility for offline security is that there has been a spill-over effect from the online world. Security measures taken by large proportions of the public include the use of high-frequency RFID technology to track the whereabouts of children and family members.[31] In homes, physical security to prevent burglaries has been stepped up. RFID tagging, although rejected in consumer articles bought in stores, is applied to household valuables and cars. In more affluent neighbourhoods, surveillance systems run by private security firms are commonplace. The more advanced systems apply facial recognition technology that matches faces of individuals with those of residents and approved visitors.[32] Individuals who are not recognised as residents or approved visitors are watched carefully and intercepted if necessary.

Vigilance and action by individual citizens and businesses have been effective in preventing some types of crimes, and the increase in individuals' recognition of their responsibilities is generally applauded. The more widespread awareness and use of online privacy and security measures seem to have prevented some cyber crimes. The numbers of crimes involving identity theft have fallen. The severity of attacks that prey on poorly fortified systems has also been reduced substantially. Publicity surrounding continued cyber threats, particularly those emanating from sources in China and India, has reinforced the view that security measures are necessary.[33] There have also been successes in tackling some

[31] Want, Roy, '*RFID: A Key to Automating Everything*', Scientific American, pp 57-65 (January, 2004).

[32] For a model of a facial recognition surveillance system see Woodward, John D. Jr., Christopher Horn, Julius Gatune and Aryn Thomas, '*Biometrics: A Look at Facial Recognition*', Annotated Briefing, RAND, 2003.

[33] Symantec, '*Symantec Internet Security Threat Report: Trends for January 1, 2003- June 30, 2003*', September 2003, http://www.symantec.com (visited on 19 December 2003), pp. 5. In the six months ending June 2003 China accounted for 5% of the total attack sources. The United States were the main source of attacks with 51% of the total.

categories of offline crime; burglaries and car thefts have been reduced and, with the help of widespread tagging, higher percentages of these crimes are solved. Offline criminals appear to be concentrating their activities to an even greater extent in poorer areas where there are more vulnerabilities.

Government Policy Responses to Demands for Privacy

Individual citizens and privacy advocacy groups, rather than government bodies, are leading the way in promoting the cyber trust and crime prevention agenda by emphasising individual security and privacy. Political parties have been responsive to demands for more privacy and have translated these demands into policy measures in their manifestos and policy programmes. In government, politicians have sought to reconcile, with varying degrees of success, the tension between the fight against crime and terrorism using the latest technological advances and the protection of individuals' privacy. Clearly, the emphasis of policy has been on the latter rather than the former. Representatives of the police and security services complain that potential gains are not being exploited and that they are losing ground in combating crime. Some in the police services regard the privacy measures as populist. However, such claims have not led to support for more police powers. On the contrary, they have given more credence to the view that members of the public need to be more vigilant and active in protecting their own security, rather than relying on public services.

Within the public sector, severe restrictions have been placed on sharing information among government bodies.[34] In conformity with strong international data-protection laws, government bodies are only permitted to use information on citizens for purposes specifically approved by the individuals concerned. Information-sharing for the purposes of crime prevention and investigation takes place on a case-by-case basis and is strictly controlled. Rules for sharing information with foreign law enforcement agencies are very restrictive, despite protests from the US. Here, federal and state law enforcement authorities are not allowed to access data about

[34] Department for Constitutional Affairs, '*Privacy and Data sharing: the way forward for public services. An update on progress*', November 2003, http://www.dca.gov.uk/majrep/datasharing/update.htm (visited on 19 December 2003); Department for Constitutional Affairs, '*Privacy and Data-sharing: the way forward*', http://www.dca.gov.uk/foi/sharing/index.htm (visited on 19 December 2003).

airline passengers' at any time, as European institutions have declared this activity to be totally incompatible with European legislation.

Restrictions have also been placed on the general availability of information held on individuals by public authorities. Individuals generally have full and easy access to the information held on them by public bodies. However, the wider availability of such information is restricted.

The proposal for a national identity card system launched in the early 00s[35] was suspended and therefore the expected benefits of this system in terms of strengthening the public sector information infrastructure were not realised. The early proposals were ambitious and foresaw a national identity register that would form the basis of the system. This register would integrate existing national insurance, tax, medical, passport, voter and driving licence records. The costs of the system spiralled beyond projections, and errors were made. During the link-up of records, there were some unfortunate incidents whereby records were matched with incorrect identities. Moreover, individual citizens were able to read other records due to the poor integration of different databases. Although these errors were detected, they undermined individuals' confidence that government could manage such a large and complex project effectively. Furthermore, due to consumer resistance, the private sector did not embrace the ID card system as expected. The ID card was not made compulsory as planned and a variety of identification forms are still widely accepted.

In conformity with new international privacy regulations, a law has been adopted restricting the length of time for which data must and can be retained. Businesses that receive personal and transactional information on their customers are obliged to preserve them only for the time required to invoice their clients and resolve any payment disputes. Free online services providing MMS and web-based e-mail are not permitted to keep any data. The data-preservation law still specifies narrowly a list of the types of data companies are able and obliged to store on their customers and the lengths of time they are permitted to store this information.[36] The

[35] Secretary of State for the Home Department, '*Identity Cards: The Next Steps*', November 2003, http://www.homeoffice.gov.uk/comrace/identitycards/ (visited on 1 December 2003).

[36] ICC, UNICE, EICTA, INTUG, '*Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes*', 4 June 2003, http://www.iccwbo.org/home/news_archives/2003/stories/data.asp (visited on 1 December 2003).

storage of customer information is not on the list. Companies require permission from customers to store information on them. Without a licence issued by the relevant privacy protection agency, operators of CCTV cameras in public spaces are not permitted to record images for longer than 30 minutes. Communication service providers operating mobile communications services are obliged to store mobile phone geopositional locations for a period of six months, after which time these records must be deleted. A limited set of public authorities, primarily the police and security services, are mandated to obtain this information on a case-by-case basis, accompanied by the appropriate legal orders. Companies complain that the data-preservation law imposes an unjustified administrative burden and that it prevents them from identifying market opportunities.

Over time, the restrictions on the availability and preservation of information have depleted the value of business services that use information held in the public and private sectors in the UK and other European countries.[37] In the US and other countries, such services continue to thrive. There, large public and private sector repositories of information are searched and systematised for information on individuals and businesses, providing companies with information on the activities of the individuals and the companies with whom they do business. In some countries, the use of background searches is now commonplace and such information services are an important business sector.

The capacity and powers of public sector data-protection and information commissioners have been expanded considerably. Privacy protection agencies have been provided with additional enforcement powers to implement laws governing information-sharing and data preservation in public bodies and in businesses. These agencies can now respond to complaints by individuals and businesses and have the authority to investigate internal processes. Moreover, new services involving the use of personal data need to be accredited by data-protection commissioners. This accreditation includes mandatory technical and operational training of all personnel.

[37] An example of such a development is the Global Regulatory Information Database (GRID) operated by Regulatory DataCorp, Int. LLC (RDC), http://www.regulatorydatacorp.com/ourServices.html#grid (visited on 5 December 2003). GRID contains approximately 1.5 million individual and business names drawn from over 22,000 international and US public record sources including government lists, media and regulatory actions.

In designing e-government services, privacy issues are a priority for government departments and executive agencies. Whether dealing with government bodies or private businesses, individuals demand that organisations adopt the available privacy-enhancing technologies and security measures. For many services, citizens demand that they are able to communicate with government bodies anonymously; for others, secure forms of authentication are required. Restrictions on the back-office integration of databases means that the forecasted efficiency gains and improvements in service delivery from e-government have not been realised.[38]

Business Responds and Adapts

Like government, businesses have also been compelled to respond to both their customers' demands for privacy and security and new national and international legislation. While there has been substantial growth in e-commerce over the past years, this has not reached the levels some expected, and there is a thriving offline retail market. Further, the way in which customers use e-commerce – in particular their reluctance to divulge information about themselves – means this is of less value than businesses had hoped. Most businesses now collect little information on the spending patterns of their British customers. Many individuals conduct online transactions anonymously using agents and e-money. In general, individuals do not want to receive unnecessary requests for information, something that they demonstrate by automatically reporting violations to their local data-protection commissioners. The costs of providing individuals, particularly high value consumers, with sufficient incentives to share information are usually prohibitively expensive, which makes it impossible to understand their preferences. Most companies find that customer relationship management systems cannot be deployed effectively in this environment. Business analysts observe, therefore, that the lack of reliable information on the spending patterns of British consumers inhibits the identification of potentially profitable markets.

[38] The benefits of IST to the provision of government services is discussed in Botterman, M. et al., '*Moving towards a Knowledge Society: the IST contribution to eGovernance*', JANUS, Joint Analytical Network for Using Socio-economic Research, May 2003, http://www.janus-eu.org (visited on 1 December 2003).

Businesses report that government monitoring of the implementation of the data-preservation law is becoming increasingly intrusive and costly since law enforcement authorities are constantly putting forward new privacy requirements as new communication technologies enter the market. Privacy protection agencies, moreover, monitor the procedures businesses have in place for obtaining the required authorisation from their customers regarding the storage and use of information. Databases held by businesses are regularly scanned by public authorities to check that unauthorised customer information is deleted within the required time periods. This situation applies also to data held abroad through outsourcing agreements, since national privacy protection agencies have signed enforcement co-operation agreements to assist each other in undertaking their tasks.

Information assurance and privacy-enhancing technologies and processes are high on corporate agendas.[39] This has been driven by customers who are highly discerning and discriminate between companies on the basis of the precautions they take on privacy and security issues. In the online world this has led to the prominence of hallmarks that guarantee the quality of security and privacy-enhancing procedures that companies bearing them have put in place. Investments have paid off in terms of reduced vulnerabilities and lower insurance premiums. However, they are also costly and constitute a barrier to entry in some markets, particularly for small firms. For instance, in the book-selling market, Amazon.com continues to occupy a strong position, and smaller firms find it difficult to establish sufficient trust among customers.

The high value that customers place on privacy has created new opportunities for certain products and services, while destroying markets for others. This was observed, for instance, during the uptake of 3G and 4G communication devices, in which the incorporation of privacy-enhancing technologies became standard.[40] This effectively prevented marketers from exploiting these communication channels to contact potential customers. For significant purchases, for example, those involving personal financial advice, the market for face-to-face services is thriving. Customers are apprehensive about disclosing the necessary personal

[39] Information Assurance Advisory Council, '*Engaging the Board: Corporate Governance and Information Assurance*', April 2003 (http://www.iaac.org.uk).

[40] Chi Haw Lee, '*Enhanced Privacy and Authentication For the Global Mobile Communications*', *Wireless Networks*, vol. 5, n.4, July 1999, pp.3-10.

information online. Online banking is popular, but customers are cautious of how they access these services and the information they disclose online. Business models that imply the ability to observe customer behaviour have not taken off. Digital Rights Management (DRM) systems that could prevent the anonymous consumption of content were a commercial failure.[41] This has forced many business people to reconsider the feasibility of their business models.

Persistent Crime Problems

Increased levels of individual responsibility for security and the related security investments by the public and private sector have not addressed important categories of online and offline crimes. While the numbers and severity of online attacks have remained fairly constant, the numbers of attempted attacks have soared, particularly from sources in China and India. For some perpetrators of cyber attacks, the increased levels of security make the challenge greater and therefore more attractive. Publicity surrounding successful and attempted attacks reinforces the view that vigilance and action by individuals and organisations are imperative. In addition, content providers claim that consumers' refusal to accept DRM technology has led to persistently high levels of theft of copyright-protected content.

Categories of offline crime not addressed by the security measures taken by individuals have continued to rise in recent years. Given insufficient public support for large-scale monitoring and surveillance by public authorities, crimes that might have been tackled effectively by such measures have remained at persistently high levels in recent years. Vandalism, assaults and shoplifting are among the offline crimes that continue to be causes for concern. Surveillance systems run by private security firms in neighbourhoods are not as effective as they might be, since they are not linked to each other nor to a central database of suspects and known criminals. RFID technology, which could be a valuable resource in preventing shoplifting, is not applied to products in high-street shops due to privacy concerns. It is speculated that some crimes have been displaced due to individuals' application of security measures: for example, from burglaries from private homes to shoplifting as a result of the use of RFID in homes.

[41] Electronic Privacy Information Center (EPIC), '*Digital Rights Management and Privacy*', http://www.epic.org/privacy/drm/ (visited on 5 January 2004).

Changes have also been observed in the types of victims targeted by criminals. As individuals have taken more responsibility for their own privacy and security, to an even greater extent than in the past victims are found in the most disadvantaged groups of society. Although online privacy and security measures are more user-friendly than ever, it still requires skills and financial resources to apply them. Further, security measures that reduce vulnerability to offline crime, such as tagging of valuables and neighbourhood surveillance systems, are not within everyone's financial reach. Reports of identity thefts have fallen, but still take place among individuals who have failed to take the appropriate precautions online. The increased concentration of offline crimes, for example burglaries in poorer areas, has also had implications for the allocation of police resources. Traditional policing methods appear to be the only available alternatives to preventing and investigating crimes in these situations.

Unsanctioned Surveillance

Actions taken by individuals to protect their privacy and security have led to increased levels of monitoring and surveillance. Examples of these developments include the use of tagging of family members and privately run local surveillance systems in homes and neighbourhoods. Critics argue that the present situation erodes privacy while failing to deliver the resources necessary to fight crimes effectively. To be of use to law enforcement, information held by individuals would need to be available to the police services in a system co-ordinated by public authorities. Privacy advocates worry that if the political climate were to change in the future, the surveillance infrastructure deployed by private individuals could be misused by government and private sector organisations. In many non-European countries, notably the US, citizens are prepared to accept far lower levels of privacy and more public and private sector surveillance.[42] While strong legislation governs the information companies are permitted to preserve on customers, there is little control over the activities of private individuals. Consequently, the most important type of surveillance, that conducted by individuals, is outside the control of government.

[42] Proposed policy measures for the US that aim to improve security and have costs in terms of privacy are found in reports by the Merkle Foundation Task Force: Merkle Foundation Task Force on National Security in the Information Age, '*Protecting America's Freedom in the Information Age*', 7 October 2002, http://www.markletaskforce.org/ (visited on 4 December 2003); Merkle Foundation Task Force on National Security in the Information Age, '*Creating a Trusted Network for Homeland Security*', 2 December 2003, (http://www.markletaskforce.org/ (visited on 4 December 2003).

Frog Boiler

Technology Uptake

During the late '00s there was an increase in the overall diffusion of IT services and technologies. After some initial failures and disenchantments, organisations have started to reap some of the benefits from those massive IT investments implemented during 2002-2005. At the same time, Internet access has become just like electricity or water: a utility. Citizens and organisations only pay for what they consume, as 'computing on demand' has been a reality since 2007. Moreover, due to new tax breaks in 2005-2006, fibre optics and digital TV have been installed in every house across the country.

Daily life has also become more wired. Mobile phones have become more 'intelligent' providing new tools and services. Having achieved 99% coverage, 3G mobile operators have become increasingly profitable. Customers, especially teenagers and university students, have been rushing to subscribe to new video-streaming services and mobile games at the same rate as people were going for GSM phones at the end of the 1990s.[43]

This success was due to a combination of three factors: First, since 2010 there has been a reduction in charges for international use of mobile phones following a successful legal case brought by the International Consumer Protection Union before the World Trade Organisation questioning the legality of roaming fees. Second, 'voice over IP' has become so common that almost 75% of fixed lines have been cancelled since normal phone calls are routed via the Internet.[44] Finally, telecom and international financial houses have been able to overcome the difficulties caused by repayment delays for the debts accrued acquiring 3G mobile licences during 2003-2005. Both have decided to work together to create a global payment system for transactions up to UK£100 since it has been in their interests to find ways to generate new revenues.[45]

[43] Ioannis Sideris, *Emerging Market Dynamics in the Mobile Services Industry*, White Paper prepared in the context of the EU-sponsored project MOBIFORUM available at http://www.mobiforum.org/mobi/documents/f_4694.PDF

[44] Upkar Varshney, '*Voice over IP*', Communications of the ACM, Vol.5, n.1, January 22, pp.89-96.

[45] Arun Bhati Slavi, '*Dial M for Money*', Proceedings of the Second International Conference on Mobile Commerce, International Conference on Mobile Computing and Networking, ACM Library, 2002, pp.95-99 and Amir Herzberg, '*Payments and Banking with Mobile Personal Device*', Communications of the ACM, Vol.46, n.5, May 2003, pp.53-58.

Consequently, since 2006, customers have been provided with access to valued-added services wherever they were in the world at limited additional costs.[46]

By 2009, the seamless wireless environment had become an established reality. Individuals now had the option to be 'always on'.[47] Their houses were 'intelligent' with Internet-based kitchen and entertainment systems. By 2010, in fact, every major household appliance had an online connection with a single Internet Protocol (IP) address thanks to the successful implementation of IPv6. By 2011, it became evident that wireless services could make money, and fears of another 'Internet bubble' soon disappeared. Wireless, in fact, was becoming big business. In 2010, TESCO plc, the world's leading supermarket chain, joined forces with SIEMENS to create the new 'automatic home food system'. By 2012, this alliance was generating about 15% of the total turnover of both companies. Similarly, in 2012, Starbucks, the US coffee-house chain, decided to take a stake in British Telecom, the UK telco owned by Hong Kong magnate Johnny Li, due to the success of its '100% Wireless Chillout Lounges'. These lounges offered customers a place to sip coffee, access a large variety of online services while listening to advertisement-free Internet radios.[48] Finally, in 2009, officials from Transport for London reached an agreement with France Telecom to provide similar services in buses and metros.

100% Online Government Services: Mission Accomplished (But with Many Problems)

Although there was a three-year delay, in May 2011 the Government announced that all public services were now available electronically. It also announced a Paper Form Elimination Bill that prohibited the use of any paper forms. Exceptions were allowed for companies operating in particularly sensitive areas such as defence and health care, as well as for physically challenged individuals. At

[46] George Giaglis et alia '*M-Business Applications and Services: Final Roadmap*' Final Deliverable EU-sponsored project MB-NET (Mobile Business Network of Excellence) at http://www.mobiforum.org/mbnet/

[47] Elisabeth Mynaat, '*Charting Past, Present and Future Research in Ubiquitous Computing*', ACM Transactions on Computer-Human Interaction, Vol.7, n.1, March 2000, pp.98-110 and Esko Kurivnen et alia, '*Understanding Contexts by Being There: Case Studies in Bodystorming*', Personal and Ubiquitous Computing, Vol.7, n.2, July 2003, pp.67-78.

[48] Eric Griffith, '*Starbucks: Your Wireless Computer Showcase*', Wi-fiplanet, 20 August 2002, available at http://www.wi-fiplanet.com/news/article.php/1449661

the core of all of these government services, there was the stipulation that every citizen and organisation had to have their own electronic signature and carry a nationally valid electronic ID card.

At first, these services worked relatively well as citizens were slowly becoming accustomed to their use. However, by 2013 the first cracks became evident. The Government, in fact, failed to properly link the distributed data-warehouses in local authorities and central government departments. Consequently, citizens were asked to provide the same electronic information over and over. Additionally, several users were able to access information about other citizens and organisations. Moreover, a new online 'underground' reality game called 'Know Your Neighbour' became increasingly popular. Developed by an Australian hacker group, the game consisted of using a piece of software that could trick UK government systems into showing other people's personal records and information stored on their electronic ID cards. Initially, these technical faults were considered unavoidable nuisances or just 'technical glitches'. After a while, however, citizens became frustrated, as they saw no adequate response from the Government to fix these problems. Some citizens even went as far as to request that the Government re-introduce paper-based transactions.

In 2014, the Government tried to counter these problems with the developers of these critical IT government systems. However, the complexity and difficulty of fixing these bugs became immediately evident. The contracts to make the UK the first country with 100% online government services had been awarded to GOV-ONLINE, a consortium of five global leading IT service providers and developers, in 2008. GOV-ONLINE had not started from scratch as it inherited those systems rushed into service between 2003-2006, many of which had been a disaster. Due to the particular nature of those contracts, the work of GOV-ONLINE did not go through the strict quality-control processes that were put in place after the IT project procurement disasters of 2003-2006. Speed of delivery was still pivotal since additional delays would have brought more embarrassment to the Government. The GOV-ONLINE consortium, therefore, was clearly told 'the sooner, the better!'

The contractors had underestimated the challenges associated with this work and its financial terms. Although several requests for contract negotiations were made, the Government was never prepared to reconsider the financial terms of the entire operation in light of its rising budget deficits. In order to stay within a manageable loss, therefore, GOV-ONLINE decided to move most of the software development for this contract to India and China by awarding pieces of the work to relatively inexperienced local subcontractors. The short-sightedness of this decision soon became evident. The selected subcontractors did not have the necessary advanced technical expertise to develop large IT infrastructures required for the integration of complex systems such as digital signatures and electronic national ID cards.[49]

Rise of Criminal Activities Using Government IT Systems

By 2015, it became evident that the technical and management weaknesses of the government online services were not just frustrating citizens. They were providing fertile ground for criminal activities. Criminals rapidly discovered that they could easily exploit these technical glitches to organise benefit fraud. At the same time, illegal schemes masquerading as consultancy and claiming to assist citizens with their electronic interaction with government became a harsh reality. Moreover, criminal organisations rapidly understood that the security vulnerabilities of the system developed by GOV-ONLINE could be easily exploited. By 2014, news reports about vast amounts of funds being syphoned from the government coffers and transferred to Vanuatu, one of the three last fiscal havens, following an unreported break-in into government networks, became a common occurrence. Some of these crimes were also facilitated by an increasing number of disgruntled employees from the large outsourcing companies responsible for managing the provision of social benefits for the Government.

During this time, the rise of computer crimes carried out through advanced computers in schools also became evident. In 2015, the Government announced the completion of the 'Fully Wired' initiative aimed at providing schools with advanced networking and wireless services. Immediately, these machines became more than important

[49] Bruce Schneier,'*IDs and the Illusion of Security*', San Francisco Chronicle, February 3, 2004, available at http://www.sfgate.com

instruments for studying; they were also a vehicle for easily exchanging copyrighted and illegal material. In some cases, students created illegal websites where it was possible to post illegal pictures taken through mobile phones. Although schools were supposed to monitor student behaviour, the technical limitations of untrained teachers become evident. On rare occasions some students were caught. It became clear, however, that when teachers discovered these illegal activities, they preferred to stay silent in order to protect the reputation of their schools.

Industry: Using IT Without Security!

By 2010, industry was finally starting to see the first tangible results of its large IT investments of the previous years. By exploiting web services and advanced Enterprise Resource Planning (ERP) tools, companies were able to manage their entire global supply chain more efficiently. These advances were also facilitated by the massive use of the new Radio Frequency Identification (RFID) technology which provided managers with a clear view of the status of supplies and sales.[50] Additionally, meta-data standards based on open specifications such as XML were now an established reality and allowed organisations to integrate their IT applications more quickly. The consumer industry had also been able to master the intricacies of Customer Relationship Management (CRM) tools. Among them, the entertainment sector had also been able to develop some initial business models to distribute its content via any type of device.[51]

Electronic and mobile commerce was also an established reality as individuals were now acquiring some goods and services online or through their wireless devices, paying through ad hoc payment systems. Financial institutions and travel services were among the industries that benefited the most and they continued to prosper. Established banks and financial houses were now providing new services and solutions to all of their individual and corporate clients at declining costs. Meanwhile, new non-financial players had also entered the market. An interesting example was 'Loans-on-a-Plate', a joint venture between SAINSBURY and HSBC, providing financial

[50] Roy Want, '*RFID: A Key to Automating Everything*', Scientific American, January 2004, pp.57-65.

[51] Thomas Messengers, '*Digital Rights Management in a 3G Mobile Phone and Beyond*', Proceedings of the 2003 ACM Workshop on Digital Rights Management, 2003, pp.27-38.

products through supermarkets and kiosks, launched in 2013. These products were instantaneously approved thanks to new software solutions based on neural network approaches. Customers were recognised through a combination of the national electronic ID and loyalty cards. Meanwhile, on the more corporate side of the financial industry, stocks and other financial products were only traded electronically through global systems. By 2016, trade, in stocks and other financial products, was primarily managed through software agents. The human role was limited to overview within the overall process.

The travel industry had also substantially changed. Tickets and travel packages were only sold via the Internet or other wireless solutions. Travel agencies had adapted themselves to provide advice to individual customers and organisations on how to manage their travel needs. Airports and seaports also changed their ways of managing passengers. Biometric solutions were now an established reality as individuals were able to board a plane or a ship without any human intervention.

Nevertheless, from 2015 it became evident that this total reliance on IT and global infrastructures was actually becoming a difficult risk to manage. As in the government sector, companies had started to notice that their networks were increasingly becoming the targets of hacking attacks. In most cases, they did not report them to national cybercrime units since this would involve lengthy investigations and the seizure of large IT infrastructures for the collection of evidence. In addition, new computer viruses or worms were unleashed on the public on a weekly basis. Gone were the days of 2004-2005 when they simply caused havoc three or four times a year. The new viruses, most of them distributed with spam email messages, were extremely virulent as they targeted almost all IT platforms irrespective of their software, changing their mode of attack and attacking a number of vulnerabilities at once. More interestingly, these were not just targeted at online services. In May 2014, a group of Mexican students had released the first worm aimed exclusively at mobile and 3G services. These young students soon realised that they had lost control of the software as millions of individual mobile phones and PDAs (Personal Digital Assistants) were infected.[52]

[52] This scenario is based on information and data collected during the EU-funded Dependability Development Support Initiative (DDSI). Final report is available at http://www.ddsi.org

Despite these malicious activities, companies continued to underestimate the risks to their IT infrastructure. As clearly indicated by Interactive Analyst, a leading global IT market research company, companies devoted, on average, only 2.3% of their IT budget to security between 2008 and 2014. The funds were expected to pay for activities such as in-house computer emergency response teams, application development and implementation, physical and IT security management, disaster recovery, business continuity and employee training. It was self-evident that these financial commitments were not sufficient to counter the risks. Companies' IT strategies were still focused on developing new services and solutions at lower costs. The only exceptions were companies operating in highly regulated industry sectors. Here, the role of chief security officer was considered important, although their main function was to prevent problems associated with national and international regulatory compliance. As clearly stated by John Charles of Interactive Analyst '... after so many years, it is evident that security is still considered as a cost and not a business benefit'.[53]

The limitations of this approach to information security became evident in 2014 when companies were increasingly unable to counter new waves of viruses and hacking attacks against wireless networks. By 2013 many businesses had moved towards wireless networks for efficiency gains. Real estate in the UK was increasingly expensive and companies could avoid the significant investment required for creating large physical networks. Nevertheless, it immediately became evident that wireless network quality of service was getting poorer by the day as a result of virus and hacking incidents.[54]

As in the case of government IT services, hackers and criminals were increasingly targeting networks for fun or profit. In November 2014 a new groups of hackers, called the 'Wireless Fighters', undertook a series of co-ordinated and simultaneous denial-of-service attacks against 'biotech' and financial businesses in Cambridge and Milton Keynes. This group, composed of students

[53] For more information see, Lawrence Gordon, '*The Economics of Information Security Management*', ACM Transactions on Information and System Security (TISSEC), vol.5, n.4, November 2002, pp.438-457 and Eugene Spafford et al, '*PFIRES: A Policy Framework for Information Security*', Communication of the ACM, vol.46, n.7, July 2003, pp.101-106.

[54] Roberto Battiti et alia, '*Global Growth of Open Access Networks: From Warchalking and Connection Sharing to Sustainable Business*', Proceedings of the 1st ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, 2003 pg. 19-28.

from local comprehensive schools, managed to take down several networks for a 24-hour period and gained access to sensitive personal information such as the DNA of specific individuals. Before finally crashing the network, a number of employees' identities were hijacked and used to access illegal material. Eventually, the group was identified when one of the perpetrators boasted of the attack in a chat room monitored by a police officer posing as a hacker. However, this was just one result against small-scale players.

In the same way that they were targeting government IT systems, criminal organisations continued to have unfettered access to unprotected company networks. In May 2015, after a long investigation, the City of London police were able to uncover a host of illegal activities undertaken by the Russian mafia. Large sums of money as well as extremely sensitive confidential data and information were stolen. Although some arrest warrants were eventually issued, the perpetrators continued to enjoy the high life by jetting between Pacific islands and other countries that had no international laws against cybercrime. Although the International Convention on Cybercrime was ratified in 2008 after three years of tortured negotiation, by 2015, there were still a significant number of nations that had not signed up to it.

On 14 November 2016, the lack of commitment by industry to security and to the need to understand their interdependencies in commercial life became truly evident. Due to a major power and communications failure in the outskirts of London, large parts of the city became severely disrupted. However, this was not the first time. People still remembered the similar problems of 2003, 2005 and 2007, although the first two were caused by terrorist attacks. However, the lessons of those events were never fully learned. As compared to previous incidents, the 2016 blackout led to massive urban violence in several areas of London. Many criminals knew that most CCTV systems did not have any emergency power systems and so they could operate with impunity. Although those that installed the cameras had to comply with certain operational regulations, most of these companies did not appear too concerned with complying with these rules, since the risk of being punished for non-compliance was very low.

Increased crime was not the only consequence of this blackout. As citizens started calling for help it become clear that most emergency communication systems, which had been privatised in 2014, were not available. After two days of violence and riots, the city started to recover but it was evident that nobody was ready to handle such massive blackouts. Blame was directed towards the government and, in particular, the police forces, since they failed to predict these events. However, it was difficult to see how they could have envisaged the real extent of the consequences.

Law Enforcement: Trying to be Active Without a Clear Agenda

By 2018, it was evident that UK police forces were unable to counter criminal activities involving new forms of IT and mobile communications technology. There were several factors that led to this situation.

The first problem was the recruitment and retention of IT-trained police officers. In 2009, the Government launched a campaigned aimed at hiring IT university students from leading universities by offering more attractive financial packages. Initially, this approach had good results. However, after three years, it became evident that most of these students preferred to move to the private sector as soon as their compulsory period ended. The private sector continued to be attractive and difficult to resist.

Money, nevertheless, was not always the reason for defection. The lack of continuous training was also a major issue. It soon became evident that those police forces dealing with IT crime needed regular and intensive training to keep up to date with technological advances. However, the available budgets could not provide the necessary resources for these activities. By 2012, the Home Office had to prioritise financial commitments to counter more pressing criminal trends such as illegal immigration, organised crime, and drug trafficking. There were attempts to counter the lack of training funds by establishing co-operation agreements with other law enforcement bodies in Europe and the United States. This led to the creation of the International Police Academy for IT crime units under the auspices of Interpol. However, by 2018 it was difficult to assess the effectiveness of this initiative, despite the fact that it created a forum for the exchange of best practices among individual members of police forces.

Law enforcement agencies were also struggling to interact with companies. By 2015, it was evident that companies were actively suspicious about reporting crimes committed against their networks. When they did, it was often too late as digital evidence was either destroyed or corrupted. This was happening even when law enforcement agencies had imposed provisions on companies operating in certain specific industry sectors, (for example, telecommunication) to retain traffic data.[55] However, the lack of information-sharing between industry and law enforcement about new IT risks and vulnerabilities was a major factor in undermining the effectiveness of law enforcement initiatives. Several schemes were attempted over the years, with the most successful being the ITSec Sharing Forum, launched in 2008. This body had the backing of all the leading UK industries and law enforcement agencies.[56]

The aim of this body was to create an electronic brokerage of confidential information about companies' IT risks and vulnerabilities and to air possible law enforcement solutions. Initially, the Forum seemed to provide the expected results. In 2009, it proudly announced that over 50 crimes were uncovered due to the sharing of information within the Forum.[57] Nevertheless, it soon became evident that the Forum was insufficient to deal with the problem. Discrepancies between national and international legislation and unclear liability regimes prevented companies from sharing information with UK law enforcement agencies. By 2015, after six years of attempts and failures, the mission statement of the forum was redrafted. The objective was now to foster the exchange of information security best practices between public and private sector organisations.

The real frustration for law enforcement was still the lack of harmonisation among cybercrime legislations. In 2015 the United Nations Cybercrime Convention was still up for ratification. Some countries were still cybercrime havens. Moreover, in 2015 there was still a lack of clear guidelines on how to collect and manage digital evidence due to rapid technology changes. The Interpol-supported International Police Academy issued some general best

[55] ICC, UNICE '*Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes*', 4 June 2003 available at http://www.iccwbo.org ; concerning forensics, see Hal Berghel, '*The Discipline of Internet Forensics*', Communication of the ACM, vol.46, n.8. (August 2003) pp.15-20.

[56] Information Assurance Advisory Council (IAAC), '*Engaging the Board: Corporate Governance and Information Assurance*', April 2003, available http://www.iaac.org.uk

[57] Rosie Cowan, Databases Tapped in Terrorist Crackdown, *The Guardian*, February 3, 2004.

practice and organised training courses for law enforcement officials and private sector IT management. However, the limited information-sharing between the experts on both sides often meant the entire exercise was of very limited value. In 2017, the academy had to finally suspend the courses due to lack of students.

Law enforcement agencies were also having difficulty in sharing information among themselves, in order to fight general crime. Although between 2005 and 2009 the Government allocated over £500 million to modernise police IT, the end result was well below expectations since there were glaring limitations in the integrity and reliability of the data. Due to national and international data protection legislation, it was difficult for law enforcement to cross-check the data with other databases. In 2010 the Government tried to pass new legislation in this area but found strong resistance among some Members of Parliament. The proposed legislation had to be rewritten and, when finally approved, was largely ineffective. The Critical Infrastructure Act was confronted with the same fate. Pushed through after the blackout of 2008, the Act soon became ineffective since its provisions applied primarily to UK-owned or based companies and did not take into consideration the data protection obstacles associated with collecting traffic and content data.[58]

Citizens: Lost in Cyberspace

After the rush towards online and mobile services of the early '00s, citizens developed an ambivalent attitude towards these technologies and services. As highlighted by Global Survey, most citizens were less and less interested. They found technology useful and, at times, necessary, if they wanted to get things done when interacting with the Government or commerce. These services were now just commodities. Online and mobile services had lost their general appeal. In May 2012, the Government tasked the Society for Future Technologies, a public/private research institution, to examine the perceptions and attitudes of citizens towards online and mobile services. The Society organised over the course of a year a large number of focus groups bringing together citizens of every age, gender, socioeconomic and cultural background across the country. The findings were extremely revealing with regard to the perceptions of citizens about technology. In particular, they

[58] Department of Constitutional Affairs, '*Privacy and Data Sharing: The Way Forward for Public Service*', November 2003 available at http://www.dca.gov.uk

emphasised their lack of trust and confidence towards these tools since they could not exercise any form of control over them. They still complained that their privacy was not protected, as confirmed by the steady rise in both email and mobile phone spam.[59] They only used the technology because they were never provided with an alternative option. The Society undertook a similar exercise two years later and saw that the mood had not really changed.

In 2013, several consumer groups had complained to the Government and police about the increasing numbers of identity thefts and spam. More importantly, they emphasised that this particular problem had already been raised in previous years and yet nothing had apparently been done to address it. The Government accepted the problem but also reminded the groups that it could not tackle the issue by itself since the direct involvement of the private sector, where most of the thefts were occurring, was required. Eventually, the two sides decided to join forces and launched a private/public partnership (PPP) called Secure Identity, the objectives of which were to teach users about how to handle their electronic identity and signature. Launched with a great fanfare, the partnership developed some initial guidelines that made it into the news. However, it soon become clear that the message was not reaching the general public due to a poor communication strategy. By 2015, the Secure Identity initiative was suspended as both the Government and industry decided to focus their efforts in other areas.

Identity was not the only concern for citizens. They had also developed a kind of invisible tolerance to the continuous rise of viruses and hacking activity against their computers. This tolerance impacted directly on technology uptake in that people used the available technology only for repetitive transactions of minor value. This was particularly evident in the case of food supply; for example, citizens had automatically programmed their fridge to order certain kind of foods and at a certain price. Nevertheless, what really concerned people was the amount of effort needed to protect themselves against fraud; to the point where one of the most successful primetime TV programmes was '*Your Daily Fraud*'. Started almost as a joke in 2009, after ten years it was still a major hit show, attracting a large number of viewers.

[59] OECD Secretariat, *Background Paper for the OECD Workshop on Spam*, Document DSTI/ICCP (2003) 10/FINAL, 22 January 2004 available at http://www.oecd.org/spam

Annex 3

Presentations Containing Modifications to the Scenarios

This annex contains the presentations of the modification to the scenarios following the discussions at the end of day 1 of each seminar game.

1. Knowing It All became Knowing What's Needed

Knowing

What's Needed

International setting

- Global Safe-Harbour Agreement for International Data Transfer
- International Data Retention Agreement for Law Enforcement
- International Alternative Dispute Resolution Systems

Awareness

- Business demands increased education/awareness from workforce
- Compulsory education in schools as soon as possible
- Raising awareness amongst consumers
- Rights and responsibilities – government to make data available to individuals

Data collection

- Citizens accept a certain level of crime to deploy resources more effectively
- Data collection and reporting reflect social and crime-prevention priorities
- Consequent optimisation of physical policing at local levels

Leave no one behind

- Recognise e.g. cash-based economy, and keep in touch with it
- Market-based solution to burden-sharing

Audit and accountability

- Establishment of an independent audit body for data access and management
- Periodic forward-looking evaluation
- Effectiveness of the independent audit body based on:
  - access to privately held data and records
  - responsible officer
  - reporting (Parliament Select Committee)

So what?

- UK is well connected
- Petty crime is at acceptable level
- Serious crime is controlled
- Government is more responsive to the people
- Situation is believed to be sustainable by all major stakeholders

2. Touch Me Not became Touch Me Gently

Touch Me Gently

Political engagement

- Opposition parties challenge the Government to lead public debate on the real costs of privacy
- Their election manifestos are centred around security as a collective responsibility
- The electorate's response puts the issue at the heart of the King's speech

International setting

- International Safe-Harbour Agreement
- International standards subscribed to by UK
- Leads to (limited) exchange of information

Empowered information commissioner

- Cyberethics Institute
  - assessing the privacy impact of new technologies
  - citizens' reporting of privacy and data protection violations by government and industry
- Information Crime Unit
- Information commissioners
  - stronger sanctions for privacy violations
  - direct co-operation with information crime unit

Awareness

- Increased education/awareness throughout society
- Compulsory education on e-literacy and e-ethics
- Raising awareness amongst consumers
- Stimulate public debate – eg Royal Commission
- Make funds available to information commissioner to counter sensationalist media reports

Information-informed consent

- People manage their own data
- Transparent and explicit use of data has prevented a situation in which government and business are not trusted with data when useful data are provided
- There is a trade-of between privacy and security. In the interest of benefiting from the knowledge available, people are happy to contribute under the right circumstances (PET, PEM) their data for international research (profiling, early warning, prosecution)

So what (crime)?

- Government has begun to re-engage
- Reporting of electronic crime at high levels; number of successful prosecutions also increasing
- The Information Crime Unit becomes a beacon for the rest of government in the way it interacts with citizens, rebuilding the relationship of trust
- UK is taken more seriously in international law enforcement circles

So what (trust)?

- Trust between individuals slowly increases
- Market for electronic data interchange and data-validation technologies increases
- Shift toward anticipatory policy-making

3. Frog Boiler became Leap Frog

Leap Frog

Awareness

- Increased education/awareness throughout society
- Compulsory education on e-literacy
- Raising awareness amongst consumers
- Government to engage with citizens and business:
  - transparent and open communication
  - advice on use of new tools
  - openness about strengths and weaknesses

Inclusion

- 100% online government services for those who want them:
  - recognition, however, that not everyone does
  - recognition that verifiable paper audit trails are sometimes the most secure and appropriate channel
- Money sits alongside virtual currencies
- Access to digital environment is viewed as entitlement for those who wish to make use of it ...
- ... but no one who wishes to stay out of the digital environment is excluded from society

Proactive planning

- Foresight programme institutionalised as triennial effort:
  - develop set of standard measures to track opportunities, threats of IT innovation
  - recommend public/private research and development pilot projects for both technology and its control
- IICM (Institute of Information Crisis Management) formed at Kings College:
  - ongoing detection, training, safe practice awareness programmes

United IT security led by business sector

- Formulates a coherent united strategy enabling business to reduce vulnerabilities:
  - backing for Secure Systems and Software Engineering computer science degrees
- Facilitates communication with government and formation of PPPs:
  - law enforcement personnel trained in business facilities
  - sharing of state-of-the-art
  - business adopts good-practice legal compliance standards

Databanks

- Central trusted third-party repository of personal data:
  - funding provided jointly by government and industry on fee basis
  - strict application of privacy control in accessing and managing data
  - strict information security management and technical controls
- Law enforcement access only through appropriate warrants
- Government indirect involvement through 'golden share'
- Reporting directly to Parliament

Assuring accuracy

- Acceptance that commonly cited information may not be the most accurate
- Regulations brought in that define where liability for information accuracy sits:
  - liability for dissemination of false information
- A minimalist policy process designed to improve levels of information accuracy:
  - the TRITE (Truth & Rebuttal for the Information Technology Environment) Council is formed to research these issues
  - search engines now throw up counter-results in addition to their normal results

International aspects

- Harmonisation of data protection
- Agreements on dependability
- Opt-in model for UK-based things:
  - data input/access
  - other standards
- World Information Organisation – 'concessions' model: standards in exchange for access, protection of laws
- Global firms: health warnings on non-compliant websites

So what?

- IICM and awareness efforts serve as a thermostat to test the temperature of the IT pot
- Internationalisation brings most countries into compliance with security standards:
  - some problem pockets continue, but they are not regarded as serious
- Criminality levels reduced by 20 per cent from 2000-2004 levels
- Business and government communities actively engage each other; citizenry

Annex 4

Description of the Case Study Subjects

Each of these subjects is a broad area of application that was used to test how participants thought the amended 2018 scenarios could play out in practice. They were chosen to highlight a number of areas where technology could have a noticeable impact.

E-Payment – a possible extension of credit card and online payment to a broad range of value transactions/transfers, from formal transactions via financial intermediaries to more informal bartering or exchange, with or without online escrow facilities. It will require dependable trustworthy systems, has to be legally enforceable across national boundaries and operate across the boundary between the physical and the virtual worlds and is dependent upon a relevant verifiable identity. Privacy is an issue as transactions may be tracked. Agent technologies may create some legal and contractual issues.

Online Medical Support – could range from sensor-based home monitoring for at-risk individuals to emergency online diagnosis and intervention management and even limited online treatment regimes. The technologies could include small sensors, perhaps attached to the body, the databases holding health records, automated drug administration and ultimately operations carried out by machines. Services would increase only as public confidence in them grows. Identity and trust will be key issues, as may the security of sensitive information. Dilemmas may occur around the priority of treatment in acute cases over establishing identity.

Customer Relationship Management (CRM) – the use by business and administration of technologies to manage long-term customer relationships in an organised way. Transaction data due to storecards has already raised privacy concerns, causing some people to start using cash again. Whilst accuracy of identity is crucial for government, business may accept out of date or partial identity information as sufficient. In the future real-time transaction, position or observation data may be used to stream marketing material to an individual via adjacent technology. Brand image may be significant for building trust here.

Forensics and Evidence – encompasses digital evidence, storage of physical evidence electronically, the potential for scene-of-the-crime evidence-gathering and acceptance within the criminal justice system. Issues include eligibility of evidence collected from machines (was the data changed by the collection process, particularly if encrypted?), security (has it been modified, audit trail?), links to identity and legal status. Disrupting and discrediting digital evidence may become a challenge for organised crime. Skill levels within the criminal justice system, beyond the forensic teams, may be important.

Road-User Technologies – may be a means of achieving environmental and societal policy outcomes. Basic requirements are probably identity of vehicle in a location, but some agencies may wish to extend to identity of driver or even passengers. Charges for road use may become relevant and time-of-day dependent. RFID type vehicle tracking devices and road-side sensors have more potential than number plate recognition, but other technologies are possible. Identity and privacy are issues, with the perceived potential for tracking to be played against safety. Legal and regulatory issues, such as enforcing insurance, vehicle safety and road tax are important and EU wide. The infrastructure may become a target for people objecting to charges etc.

Provision of Benefits – an example of a government service dependent upon verifiable identity, though often claimants may lack technology or social skills and are therefore vulnerable to crime. Balancing need against provision is a challenge for agencies, particularly for at-risk groups. The security of any central database will be a privacy concern, as data held could be valuable to credit agencies etc. Online systems may help agencies ensure that eligible people claim benefit. Biometrics and entitlement cards could be relevant technologies.

Annex 5

Lessons Learnt from the Case Study Subjects

Knowing What's Needed

Lessons learned from the case studies

Know: Benefits

- Benefits payment is a form of connection:
  - to the wired world (familiarity with equipment, use of e-payment, etc.)
  - with the public world (use public POP if ID card exists, require periodic contact with DWP clerks, etc.)
  - with the taxpaying world
- E-benefits may be highly efficient:
  - possibility of 'horribly fair' system
  - more efficient payment (higher cost – backlash)
  - better targeting, incentives
- E-benefits may be more frustrating:
  - machine rage
  - need for 'digital advocate'
- May increase 'digital refuseniks' (among claimants or an inversion: middle-class opt-outs, wired underclass)
- Long-term shift in understanding of purpose of benefits

Know: CRM

- Distinction must be made between customer and citizen
- Business will accept a lower level of accuracy than government
- Increased public awareness would mean that market could be left to regulate itself
- Separate databases rather than one centralised database would provide safeguards
- International audit standards required

Know: E-Payment

- Maintain customer choice when rolling out e-payment systems
- Emphasise value to individuals in terms of convenience
- Accept existence of non-e methods of payment
- Facilitate range of e-payment methods with varying degrees of anonymity
- Stay alert for new crime opportunities

Know: Forensics and Evidence

- Who will police the police? New role for PITO to audit police use of technology?
- Data will be stored in numerous locations – no longer a question of seizing hard drive
- Partial identities will be of dubious evidential value
- Specialist training for judiciary required
- Over-reliance on digital evidence to be avoided

Know: Online Medical

- Keep personal consultations to obtain maximum benefits
- Ensure choice regarding storage of personal data:
  - patients should always have access to own records
- Address issues of use of data by insurers and researchers
- Prepare for new and redefined roles for health care professionals:
  - including monitoring performance of GPs and hospitals

Know: Road User

- Puts different purposes of road charging (revenue, safety, congestion, time-of-day smoothing etc.) into sharp relief
- Does this undermine the model of the road as a commons?
- Concerns over fairness – different groups need different amounts of use (parents, workers, rural residents)
- Does a charge tied to vehicle, place and time capture WTP and social cost? (what about purpose, occupancy)
- Will acceptance diffuse through cities?
- The patterns of traffic, land use, road layouts, etc. may look very different:
  - a result of enhanced e-working, e-commerce
  - need for charging may vanish
  - tollbooth, tradable charging devices may be superior

Know: Road User (cont.)

- Overall feeling that petrol tax may be simpler and more acceptable, but that charging scheme can be targeted more precisely
- Group felt that if this was implemented, democracy must be 'off the agenda'

Touch Me Gently

Lessons learned from the case studies

Touch: Benefits

- These are complex systems that we cannot continue to patch
- We need a fundamental rethink of the way money moves (in both directions) between government and citizens
- Incremental simplification

Touch: CRM

- Government should not view citizens as customers
- Principle of informed consent for the citizen/customer about the control of personal data
- Need for better IT to allow individuals to better manage their data

Touch: E-Payment

- Need dependable payment infrastructures
- Universal service provision on the part of banks (under government regulations)
- Recognise and foster diversity of provision

Touch: Forensics and Evidence

- Trade-offs between privacy and security needs to be explicitly made according to utilitarian principles
- Must address problems of location and admissability of evidence
- Must address problems of understanding of evidence arising from complexity of information

Touch: Online Medical

- Need broad public debate on ethics
- Need transparency of data use for research purposes
- Divulgence of information needs to be done according to a clear and explicit contract

Touch: Road User

- Track the vehicle, not the individuals, and everything else will follow
- Government must demonstrate trustworthiness in limiting surveillance
- There must be tangible, clearly explained, demonstrable benefits to the individual
- Surveillance and security may not be mutually exclusive

Leap Frog

Lessons learned from the case studies

Frog: Benefits

- We interact with and trust supermarkets more than government
- Don't buy into universal (anything) that the technologists tell you
- Usability – the system will be electronic but interfaces will be multi-modal:
  - paper, television, voice, electronic
- Abusability – open to fraud by government and business (need multiple levels of security and trusted governance)
- Accessibility – let the user control where and when

Frog: CRM

- ID cards would have a symbolic psychological value over and above their practical utility
- This is a good way to accomplish the leap forward from 2004 to 2018:
  - people need tangible representation of their identity
- System must not be compulsory:
  - this is fundamental to establishing trust
- Identification of sensitive data is contextual:
  - one size does not fit all
  - today's sensitive may be tomorrow's commonplace (both societally and individually)

Frog: E-Payment

- e-cash has both costs and benefits:
  - anonymity – itself a two-edged sword
  - opportunities for criminal activity
  - cost of maintaining parallel systems
- Institutions don't change much from 2004:
  - relationships with TTPs not very different
  - there will always actors outside the regulatory system
- Fraud happens:
  - but likely to be only on a small scale (but perhaps large volume)
  - this leads to potentially unstable system

Frog: Forensics and Evidence

- A difference between forensics and evidence:
  - volume of forensics will increase
  - what is considered admissible evidence may decrease as standards of proof change
- Evidence in order to be acceptable needs to be:
  - valid
  - accurate
  - relevant ('Bramley rules')
  - acquired in a legitimate way
  - subject to review

Frog: Online Medical

- Use citizen push and administration/ business pull to encourage take-up
- Ensure that access is set by user, but with overrides that follow legal process
- Avoid misuse of medical information
- Behavioural control through technology

Frog: Road User

- Probably can't impose charging
- Market mechanisms might work (what 'tariff' do you want for your car?)
- Need to think through the potentially serious unintended consequences:
  - e.g. uncertainty, data re-use, emotional backlash
- Creeping taxation and mechanism to ratchet up taxes
  - no opposition to paying, just to increases for no reason

Printed in the UK on recycled paper with a minimum HMSO score of 75.
First published June 2004. Department of Trade and Industry. www.dti.gov.uk