MULTI-DISCIPLINARY ISSUES

INTERNATIONAL FUTURES PROGRAMME

OECD/IFP Project on

"Future Global Shocks"

"Reducing Systemic Cybersecurity Risk"

Peter Sommer, Information Systems and Innovation Group, London School of Economics

Ian Brown, Oxford Internet Institute, Oxford University

January 2011

NOTE: This document is under embargo until 17 January 2011. The document contains an unofficial copy of a report for the purpose of informing media sources in advance of its official release. Slight differences may appear between the issue of this unofficial copy and the time it appears on the website of the OECD International Futures Programme on 11 June 2010. The opinions expressed and arguments employed herein are those of the authors alone, and do not necessarily reflect the official views of the OECD or of the governments of its member countries.

Contact persons:

Pierre-Alain Schieb: +33 (0)1 45 24 82 70, Pierre-Alain.Schieb@oecd.org

Anita Gibson: +33 (0)1 45 24 96 27, Anita.Gibson@oecd.org

Executive Summary

This report is part of a broader OECD study into "Future Global Shocks", examples of which could include a further failure of the global financial system, large-scale pandemics, escape of toxic substances resulting in wide-spread long-term pollution, and long-term weather or volcanic conditions inhibiting transport links across key intercontinental routes.

The authors have concluded that very few single cyber-related events have the capacity to cause a global shock. Governments nevertheless need to make detailed preparations to withstand and recover from a wide range of unwanted cyber events, both accidental and deliberate. There are significant and growing risks of localised misery and loss as a result of compromise of computer and telecommunications services. In addition, reliable Internet and other computer facilities are essential in recovering from most other large-scale disasters.

- Catastrophic single cyber-related events could include: successful attack on one of the underlying technical protocols upon which the Internet depends, such as the Border Gateway Protocol which determines routing between Internet Service Providers and a very large-scale solar flare which physically destroys key communications components such as satellites, cellular base stations and switches.
- For the remainder of likely breaches of cybsersecurity such as malware, distributed denial of service, espionage, and the actions of criminals, recreational hackers and hacktivists, most events will be both relatively localised and short-term in impact.
- Successful prolonged cyberattacks need to combine: attack vectors which are not already known to the information security community and thus not reflected in available preventative and detective technologies, so-called zero-day exploits; careful research of the intended targets; methods of concealment both of the attack method and the perpetrators; the ability to produce new attack vectors over a period as current ones are reverse-engineered and thwarted. The recent Stuxnet attack apparently against Iranian nuclear facilities points to the future but also the difficulties. In the case of criminally motivated attacks: a method of collecting cash without being detected.
- The vast majority of attacks about which concern has been expressed apply only to Internet-connected computers. As a result, systems which are stand-alone or communicate over proprietary networks or are air-gapped from the Internet are safe from these. However these systems are still vulnerable to management carelessness and insider threats.
- Proper threat assessment of any specific potential cyberthreat requires analysis against: Triggering Events, Likelihood of Occurrence, Ease of Implementation, Immediate Impact, Likely Duration, Recovery Factors. The study includes tables with worked examples of various scenarios

- There are many different actors and with varying motivations in the cybersecurity domain. Analysis and remedies which work against one type may not be effective against others. Among such actors are: criminals, recreational hackers, hacktivists, ideologues, terrorists, and operatives of nation states.
- Analysis of cybsersecurity issues has been weakened by the lack of agreement on terminology and the use of exaggerated language. An "attack" or an "incident" can include anything from an easily-identified "phishing" attempt to obtain password details, a readily detected virus or a failed log-in to a highly sophisticated multi-stranded stealth onslaught. Rolling all these activities into a single statistic leads to grossly misleading conclusions. There is even greater confusion in the ways in which losses are estimated. Cyberespionage is not a "few keystrokes away from cyberwar", it is one technical method of spying. A true cyberwar is an event with the characteristics of conventional war but fought exclusively in cyberspace.
- It is unlikely that there will ever be a true cyberwar. The reasons are: many critical computer systems are protected against known exploits and malware so that designers of new cyberweapons have to identify new weaknesses and exploits; the effects of cyberattacks are difficult to predict – on the one hand they may be less powerful than hoped but may also have more extensive outcomes arising from the interconnectedness of systems, resulting in unwanted damage to perpetrators and their allies. More importantly, there is no strategic reason why any aggressor would limit themselves to only one class of weaponry.
- However the deployment of cyberweapons is already widespread use and in an extensive range of circumstances. Cyberweapons include: unauthorised access to systems ("hacking"), viruses, worms, trojans, denial-of-service, distributed denial of service using botnets, root-kits and the use of social engineering. Outcomes can include: compromise of confidentiality / theft of secrets, identity theft, web-defacements, extortion, system hijacking and service blockading. Cyberweapons are used individually, in combination and also blended simultaneously with conventional "kinetic" weapons as force multipliers. It is a safe prediction that the use of cyberweaponry will shortly become ubiquitous.
- Large sections of the Critical National Infrastructure of most OECD countries are in not under direct government control but in private ownership. Governments tend to respond by referring to Public Private Partnerships but this relationship is under-explored and full of tensions. The ultimate duty of a private company is to provide returns for its share-holders whereas a Government's concern is with overall public security and safety.
- Victims of cybersecurity lapses and attacks include many civilian systems and for this reason the value of a purely military approach to cybsecurity defence is limited. The military have a role in protecting their own systems and in developing potential offensive capabilities.
- Circumstances in which the world or individual nations face cybersecurity risks with substantial long term physical effects are likely to be dwarfed by other global threats in which information infrastructures play an apparently subordinate but nevertheless critical role. During many conventional catastrophes there is a significant danger that a supportive information infrastructure becomes overloaded, crashes and inhibits recovery.

- The cyber infrastructure, as well as providing a potential vector for propagating and magnifying an original triggering event, may also be the means of mitigating the effects. If appropriate contingency plans are in place, information systems can support the management of other systemic risks. They can provide alternate means of delivering essential services and disseminate the latest news and advice on catastrophic events, reassuring citizens and hence dampening the potential for social discontent and unrest.
- Rates of change in computer and telecommunications technologies are so rapid that threat analyses must be constantly updated. The study includes a series of projections about the future.
- Counter-Measures need to be considered within an Information Assurance engineering framework, in which preventative and detective technologies are deployed alongside human-centred managerial policies and controls.
- A key distinguishing feature of cyberattacks is that it is often very difficult to identify the actual perpetrator because the computers from which the attack appears to originate will themselves have been taken over and used to relay and magnify the attack commands. This is known as the problem of attribution. An important consequence is that, unlike in conventional warfare, a doctrine of deterrence does not work – because the target for retaliation remains unknown. As a result, defence against cyberweapons has to concentrate on resilience – preventative measures plus detailed contingency plans to enable rapid recovery when an attack succeeds.
- Managerial Measures include: risk analysis supported by top management; secure system procurement and design as retrofitting security features is always more expensive and less efficient; facilities for managing access control; end-user education; frequent system audits; data and system back-up; disaster recovery plans; an investigative facility; where appropriate – standards compliance
- Technical Measures include: secure system procurement and design; applying the latest patches to operating systems and applications; the deployment of anti-malware, firewall and intrusion detection products and services; the use of load-balancing services as a means of thwarting distributed denial of service attacks
- Large numbers of attack methods are based on faults discovered in leading operating systems and applications. Although the manufacturers offer patches, their frequency shows that the software industry releases too many products that have not been properly tested.
- Penetration Testing is a useful way of identifying system faults
- Three current trends in the delivery of ICT services give particular concern: World Wide Web portals are being increasingly used to provide critical Government-to-citizen and Government-to-business facilities. Although these potentially offer cost savings and increased efficiency, over-dependence can result in repetition of the problems faced by Estonia in 2007. A number of OECD governments have outsourced critical computing services to the private sector; this route offers economies and efficiencies but the contractual service level agreements may not be able to cope with the unusual quantities of traffic that occur in an emergency. Cloud computing also potentially offers savings

and resilience; but it also creates security problems in the form of loss of confidentiality if authentication is not robust and loss of service if internet connectivity is unavailable or the supplier is in financial difficulties

The authors identify the following actions for Governments:

- Ensure thatnational cybersecurity policies encompass the needs of all citizens and not just central government facilities
- Encourage the widespread ratification and use of the CyberCrime Convention and other potential international treaties
- Support end-user education as this benefits not only the individual user and system but reduces the numbers of unprotected computers that are available for hijacking by criminals and then used to mount attacks
- Use procurement power, standards-setting and licensing to influence computer industry suppliers to provide properly tested hardware and software
- Extend the development of specialist police and forensic computing resources
- Support the international Computer Emergency Response Team (CERT) community, including through funding, as the most likely means by which a large-scale Internet problem can be averted or mitigated
- Fund research into such areas as: Strengthened Internet protocols, Risk Analysis, Contingency Planning and Disaster Propagation Analysis, Human Factors in the use of computer systems, Security Economics
- Attempts at the use of an Internet "Off" Switch as discussed in the US Senate and elsewhere, even if localised, are likely to have unforeseeable and unwanted consequences.

Systemic Cyber Security Risk

This study is part of a broader OECD research project on Future Global Shocks. It asks: "How far could cyber-related hazards be as devastating as events like large-scale pandemics and the 2007-10 banking crisis?"

Significant interest in the potential of cyber-related disaster can be dated back at least to the mid-1990s with reports such as the US *Security in Cyber-Space* (GAO, 1996) and Winn Schwartau's book *Information Warfare: Chaos on the Information Superhighway* (Schwartau, 1994). Back in 1991 Jim Bidzos from the security company RSA had originated the much-repeated phrase: "Digital Pearl Harbor". There was another peak of concern in 1998 and 1999 over fears of the Y2K bug – the concern that older computers had not been programmed to cope with date presentation in the up-coming millennium and would crash. Interest then faded somewhat until 2007 when Estonia suffered from a number of cyber attacks.

Between the early 1990s and now, the Internet, the ways in which it is used, the commercial and social infrastructures associated with it, and the numbers and types of people who use it, have changed out of all recognition. To only a slightly lesser extent there have also been profound changes in non-Internet computer and telecommunications technologies and these have impacted on theday-to-day routines of individuals, commercial organisations, NGOs and governments .

The Estonian events were followed by online attacks during war-like skirmishes in Georgia and the Middle East, allegations of large-scale industrial espionage and reinforced by indications that organised crime had "gone cyber". Breach of critical telecom cables, almost certainly accidental, also pointed to potential physical triggers for high-impact loss of connectivity.

By 2009 NATO had set up a centre of excellence in cyberdefence in Estonia, and the following year the United States spoke of having a Cyber Command. It already had a White House-based cybersecurity advisor, The United Kingdom set up an Office of Cyber Security (later renamed the Office of Cyber Security and Information Assurance) and also a Cyber Security Operations Centre. At a European level there was ENISA – the European Network and Information Security Agency.

The history of the subject that used to be called "computer security" can be traced back to the late 1950s; books on "Computer Crime" started to appear in the early 1970s. But most individual instances of data corrupted and computers crashed by "malware" (malicious software), computer-aided financial fraud, extortions, identity theft, spam distribution, web defacements and commercial espionage activities have had, in global terms, limited impact, however distressing for victims.

The test we have applied in this study is for a potential "global shock". Candidates are considered elsewhere in this broader OECD study: in a pandemic enough people fall ill simultaneously to the point where there are insufficient well individuals to staff essential services such as transport, primary and hospital healthcare, provision of water, power, fuel, etc and to provide basic policing. From the trigger of the illness there could be a cascade of events into social breakdown which crosses national boundaries. Similarly, the 2007 banking crisis was set off by a mistaken reliance by financial institutions on the value of derivate debt instruments based on sub-prime mortgages. Because so many large financial institutions had made the same error and committed such large portions of their assets, once the bubble had burst, they could no longer meet their obligations. The problem became

global because loss of confidence in one institution triggered the same in others. Moreover these were the same institutions that were providing routine cash-flow finance for very large numbers of hitherto stable businesses. When these businesses could no longer operate, they had to lay off staff. The newly unemployed had less money to spend so that other businesses suffered reductions in economic activity. The stock market value of many businesses fell, impacting among others on the values of the pension funds and their ability to support retirees.

One important characteristic of a global shock is that responses limited to the level of the nation state are likely to be inadequate; coordinated international activity, with all the associated problems of reaching agreement and then acting in concert, is what is required.

But other headline-grabbing events, though having profound local effects and prompting charitable responses, are not in the same way "global" shocks. The Haiti earthquake of January 2010 is in this category, largely because in global terms Haiti is not economically significant. The same could be said of the all-too-frequent floods in Pakistan and Bangladesh and famine due to drought in parts of Africa. These have considerable local, but not global, impact. The ash from the Eyjafjallajökull volcano in Iceland in April 2010 might have become a global shock had the authorities maintained their initial orders for large no-fly zones.

The Mexican Gulf oil spill also of 2010 occupies a marginal position: it was disastrous for the inhabitants of Louisiana and Florida – but also affected pensioners in the United Kingdom because of the extent of their indirect – and often unaware – investment in BP.

Where, in a period of heightened concern about their range and scope, do cyberthreats rank?

Analysts and researchers soon become aware of some problems. The first is that despite a multiplicity of potential triggering events – hardware based, software based, accidental, deliberate– it turns out that there are very few single cyber-events with the capacity to provoke a global shock. There are, however, rather more situations in which combinations of events may trigger a cascade, for example when two or more cyber events take place simultaneously, or a cyber event coincides with a more conventional disaster. Circumstances in which the world or individual nations face cybersecurity risks with substantial long term physical effects are likely to be dwarfed by other global threats in which information infrastructures play an apparently subordinate but nevertheless critical role. During many conventional catastrophes there is a significant danger that a supportive information infrastructure becomes overloaded, crashes and inhibits recovery. From the public's point of view the absence of a clear government response may trigger panic if there appears to be no route back to normalcy.

The second problem is that of evaluating the available anecdotes and accounts of alleged events. How accurate and thorough has been the analysis of the causes and the amount of actual damage? Linked to this is a third problem: a lack of agreement on terminology. It soon becomes obvious that, among the various writers and producers of statistics notions of what amounts to an "incident", an "attack", even "cyberwar", vary considerably. In individual surveys in which large numbers of potential victims have been asked about their experiences there is often doubt that every respondent has used the same definition.

Next, we must recognise that there are a variety of motivations behind those who seek initiate a destructive cyber-event – and recognition of this is important in devising responses and counter-measures. For example, a cyber criminal or terrorist cannot be deterred from using cyber attacks in the same way as a nation state. If someone commits cyber fraud (a criminal act) or disables critical infrastructure with a virus (a criminal and potentially terrorist act), law enforcement will do what it can to find and prosecute the individual or

group involved. If a State causes damage to another State with a cyber attack which arises to the level of war, then it risks retaliation with kinetic weapons.

Problems of Definition

If you decide to include every occasion when an anti-malware program successfully detects a virus or Trojan and every time when an Intrusion Detection System registers a potentially aggressive probe and every time a phishing attempt is received, you can produce statistics that show that there are multiple attacks even on small insignificant computer systems every hour of every day. Alternatively if you only count events that have been the subject of successful criminal convictions, the quantity of cyberattacks is vanishingly small. Most analysts seem to adopt variable definitions between these two extremes. There is also scope for dispute whether to include physical attacks that are largely aimed at disabling computers and their associated infrastructure.

Problems of Estimating Loss

Few of the cost estimates for "cyberhazards", "cyber incidents", "cyberattacks" or "cyberwarfare" explain key assumptions. As there is seldom much in the way of physical loss, the immediate direct losses are often very low. But how far do you include remedial costs, particularly if part of those go to the installation of detective, preventative and mitigating technologies that should have been there in the first place? Looking more generally at the consequential losses, what are the criteria for inclusion? For example, an insurer might be prepared to pay out for provable loss of revenue (based on a previous year's business records), but not for a lost business opportunity (if only my computer had been working my presentation might have won me a valuable new contract). For businesses there may also be reputational losses. In a wider event there is also the problem of looking at losses from the perspective of who pays for them. For example, if you have a valid insurance policy and incur a covered loss – you will be compensated for most of that loss while it could be said that paying out on claims is a normal part of an insurer's business. Estimates of annual global losses attributable to cyber events or cybercrime are even more problematic as there is no guarantee that all possible victims have been polled, or that they have provided detailed responses. In 2004 Cashell and others wrote a report on *The Economic Impact of Cyber-Attacks* for the US Congressional Research Service which raises still further ways in which loss could be measured. (Cashell, 2004)

Defining Cyberwar

The phrase "cyberwarfare" acquired a considerable revival of interest in 2008 - 2010, though earlier phrases such as "information warfare" also appear in the mid 1990s. The word seems to be used in a number of different ways. Some writers refer to a war conducted substantially in the cyber or virtual domain. Those with this type of perception are often of the mindset that cyber wars are likely to be very similar to conventional or "kinetic" wars and that similar military doctrines of retaliation and deterrence are likely to hold sway.

It is much easier to define "cyberwar" as the tests are the same as for any conventional "kinetic" war. Some of the key international treaties include the 1899 and 1907 Hague Conventions, 1945 UN Charter, 1948 UN Genocide Convention and the 1980 UN Convention on Excessively Injurious Conventional Weapons. In essence, to decide whether an act amounts to cyberwar one applies a test to see whether it was "equivalent" to a conventional hostile attack and looks to scope, intensity and duration. There is also a distinction between acts aimed at military and civilian targets.

The UN Charter addresses the required justification for counter-measures for those who claim to have been attacked. Essentially, the victim has to be able to produce reliable evidence of who had been attacking (not always easy in the cyber world) and the effects of the attack. The aim of countermeasures must be to force an attacking state to meet its general obligations under the UN Charter (Article 49). (NRC: 2010). However, this concept of "cyberwar" would seem to apply only to nation states, not to sub-state actors. It would also exclude large-scale cyber-espionage.

It is for these reasons that it can be argued that the focus of analysis should be on the capabilities of the various forms of **cyberweaponry**. The primary concern should be the reasons why someone may want to go to war or indulge in hostile activity less than full-scale warfare. These would typically be disputes over territory, disputes to assert hegemony, disputes over access to resources and raw material, disputes over religion, and historic disputes and revenge. Once hostilities exist there seems to be little reason why states would limit themselves to kinetic weaponry. Cyberweaponry simply provides additional means by which the hostility can be advanced.

A fifth issue is the speed of change in computer and communications technologies and the effects these have on economic, social and cultural structures. It means that historic events may not offer much guidance about what could happen in the future. Any sensible analyst will be wary of projecting scenarios too far into the future.

In any broader analysis of potential national and global "shocks" it has to be recognised that the cyber infrastructure, as well as providing a potential vector for propagating and magnifying an original triggering event, may also be the means of mitigating the effects. If appropriate contingency plans are in place, information systems can support the management of other systemic risks. They can provide alternate means of delivering essential services and disseminate the latest news and advice on catastrophic events, reassuring citizens and hence dampening the potential for social discontent and unrest.

The structure of this study is as follows. The first section describes the risk and its historical context. This includes the growing dependence of individuals, institutions and governments on critical information infrastructures such as the Internet. This section also covers the anticipated use of these infrastructures in contingency planning – how disasters are anticipated and planned for and the processes involved in recovery from catastrophes.

The second section characterises the different types of systemic cybersecurity risks. These include accidents affecting infrastructure, deliberate attacks, system overload and espionage. Although there is some overlap in such a taxonomy, in each instance we indicate the main preventative and remedial routes and describe different models for risk analysis.

The third section looks at a series of typical scenarios. Some are based on recent events while others arise out of reasonable forecasts. Most are elaborated in two extensive appendices, which also seek to contribute insights to evaluating the risks in terms of, amongst other factors, propagation and longevity.

To better understand the processes, mechanics and feasibility of recovery, a fourth section examines preparedness in government and the private sector, regulatory frameworks, international co-operation, co-operation between different entities within nation states and public communication.

The final section presents conclusions and recommendations. Contrary to much recent writing, single hazards and threats in the cyber domain will probably not propagate into a

full-scale global shock. However there are several plausible scenarios which if realised will have significant impact at the level of the nation state as well as causing long-term damage to businesses and individuals. A pure Cyberwar, (wherein only cyberweaponry is deployed) is unlikely. Future wars and the skirmishes that precede them will involve a mixture of conventional or kinetic weapons with cyberweaponry acting as a disrupter or force multiplier.

Downplaying the concept of Cyberwar also implies that armed forces have a relatively limited role in protecting nation states against cyber threats. Whilst the military undoubtedly rely on computers and networks for their own operations and obviously need to protect them, many of the victims of cyber attacks, or of outages of essential services dependent on the Internet and computers, are and will be substantially civilian. Thus, greater emphasis on governmental "civil contingencies" programmes and a more thorough examination of some of the tensions within so-called Public Private Partnerships is desirable. More detailed recommendations are provided about the prospects for international co-operation, objectives for further research, and the role of law and education; both to produce a cohort of skilled technicians, but also to educate potential victims.

Readers should be aware that computer and communications technologies continue to evolve at a very fast pace. In general, long-term hardware and demographic trends are more predictable than those related to software and social change. Establishing the facts of certain crimes and other events may also be difficult: investigations can be technically challenging and cross national boundaries, and victims may prefer to conceal losses to protect their reputation rather than cooperate with law enforcement agencies. There is a considerable difference between the effects of "possible" and "likely" scenarios.

Description and historical context

We begin with a brief historic overview of developments in computing and their impact on the global risk landscape. Over the last 50 years there has been a continual increase in levels of sophistication, dependency, expectations, inter-connectedness and just-in-time delivery of services. Within each there are changing patterns of risk and opportunities for cyber-based disasters. These trends can be expected to continue, though the precise ways in which they will interact is difficult to predict over the longer term.

Early days of business and government computing

By the mid-1950s a number of large businesses and government agencies had established Electronic Data Processing (EDP) departments to automate and speed up clerical tasks. Computing was done in "batch jobs" rather than in "real-time". The main risks were of electro-mechanical breakdown and poor programming.

By the 1970s the costs of computing had fallen dramatically. Hardware was cheaper; smaller companies could purchase computer-time from bureaux; and there was the beginning of a market for software independent of hardware suppliers. There were also the beginnings of real-time computing, where a user could get an instant response to a query from a computer rather than waiting for a batch-generated report. Computer failure was still a risk, and because more people had access to the computers and to data input and output there were opportunities both for fraud and data theft. Organisations that acquired significant computing resources were able to dispense with some clerical and administrative staff.

The growth of real-time, interactive computing led to the development of operating systems such as MULTICS that allowed simultaneous users and processes. From this pioneering development came concepts such as password-protected accounts for individual users, which provided some assurance that a specific individual was at a terminal at a particular time – still an essential feature of computer security.

1970s and 1980s: changing patterns of risk

During the later 1970s and 1980s these trends continued. Computers were used to generate reports and analyse customer needs, production processes and cash flows. Businesses reorganised themselves internally: many middle managers and clerical staff were no longer needed. Computer-derived information helped businesses become more efficient

In the mid-1970s specific data networks began to appear. Initially there were a number of incompatible proprietary networks, operated by very large computer and telecommunications companies. Customers began to create industry-based networks within which messages and other data could be exchanged. Financial service providers were an early adopter. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) was conceived in 1973, went live in 1977 and had passed 10 million messages by the end of its first operational year (SWIFT, 2009). The messages passed on such networks could be formal instructions, informal e-mails and even contractual requirements. These networks spread to other industries, which set up Electronic Data Interchange systems to order goods and services.

The growth of proprietary networks had relatively limited impact on the risk profiles of most organisations, as unauthorised access to the networks was physically and technically difficult. Increasing numbers of people entered the computing industry, but were mostly IT professionals or clerical "data input" staff. The population of potential computer criminals was very limited. Access to computers was usually via the premises of organisations that owned or leased them. Outside access using dial-up modems was possible, but such

equipment was expensive and rare. As a result attacks from the population at large were almost unknown.

The greatest risk was fraud. The most common technique involved gaining unauthorised access to an official computer terminal within an organisation and issuing an order for payment or release of goods. A sophisticated version of this was used in 1978 to arrange wire transfers from the Security Pacific Bank for some US$ 10 million. There were some examples of frauds involving direct manipulation of computer data – in the Equity Funding Corporation scandal of 1973, a failing investment company sought to mask its difficulties by re-running its records to create a whole series of apparently valuable accounts which could then be sold on to third parties for cash (Cornwall, 1988). Industrial espionage via access to computers was more of a theory than a practical reality because, at that stage, there were relatively few industrial secrets committed to computers. Sabotage aimed at stopping a computer working consisted largely of physical attacks on computer equipment (Wong, 1983). Typical examples included the use of bombs and guns but also, more mundanely, the judicious insertion of a screwdriver to short-out a circuit board or damage a mechanical part.

The first books on computer security – both for professionals and for the general public – appeared in the 1970s and marked the first public recognition of a security problem.

Routes to democratisation

By the end of the 1980s the personal computer in the home and on the corporate desktop was no longer an oddity. Many terminals had modems for external communication. There were many more self-taught computer users.

This period also saw the emergence of recreational hackers – those who liked to devise technology-based jokes or to explore networks. Among the "jokes" were the first instances of malicious software or "malware" - viruses that were spread from PC to PC when floppy disks, then the easiest form of data transport, were inserted.

During the early 1980s hobbyists with modems succeeded in breaking into corporate and government computers that offered dial-up access to their employees. Some hackers discovered dial-up facilities that gave them access to international networks. Knowledge of how to access "interesting" computers and networks was spread via various online bulletin boards.

The costs of business computing fell, so many more organisations bought their own computers. The range of applications expanded to include specialist tools such as Computer Aided Design and extensive customer databases. Security awareness did not develop at the same speed as the rest of computing, so there was greater scope for fraud and new opportunities for industrial espionage.

The changing demographics of those with access to computers and networks meant that there were new opportunities for those of a criminal inclination and also that less skill was required to take advantage of the new environments.

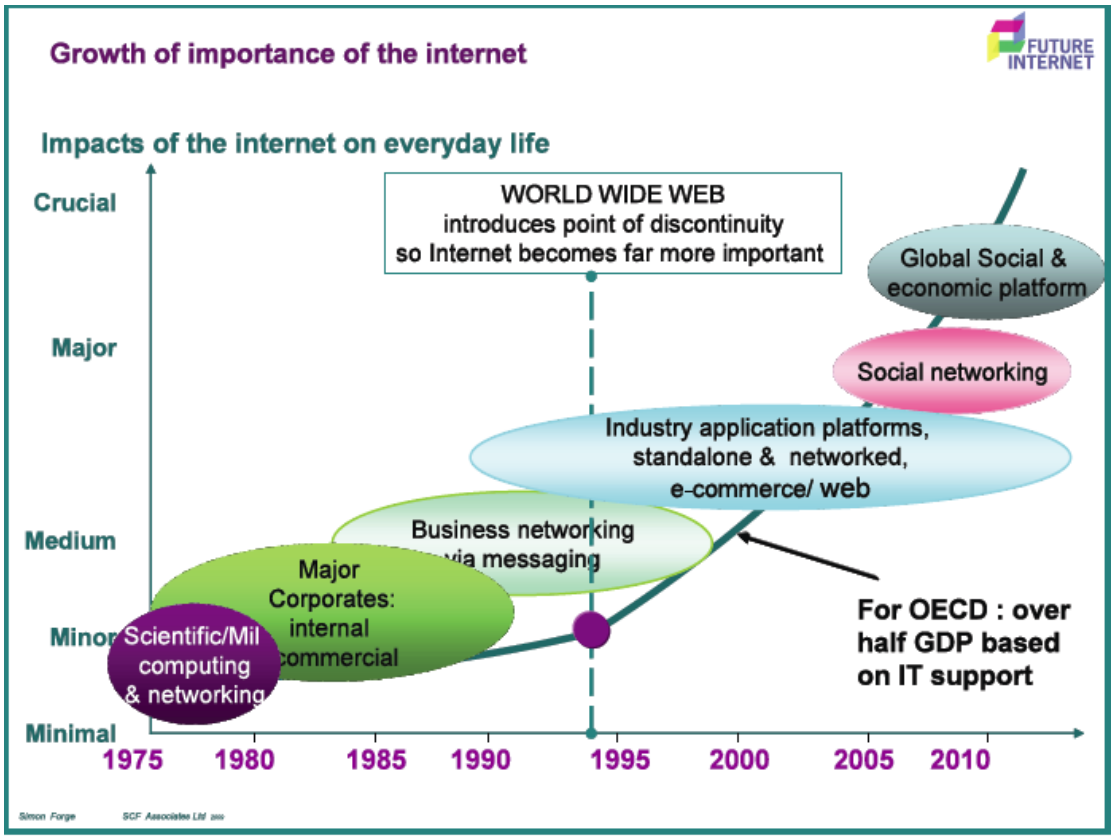
A further feature was that installing and maintaining computers ceased to be the preserve of a highly trained engineering elite. The more casual use of computers, together with their increasing sophistication, meant that there were greater opportunities for debilitating flaws to occur and not be noticed until the damage was manifestly apparent.

The emergence of the Internet

The Internet developed slowly at first. From the late 1960s until the late-1980s, it was mainly a research network that linked universities and government bodies. The development of the World Wide Web in the early 1990s brought increasing numbers of non-academic users. Between 1993 and 1995 the Internet was fully opened to commercial traffic. By 1996 it connected over 15 million machines.

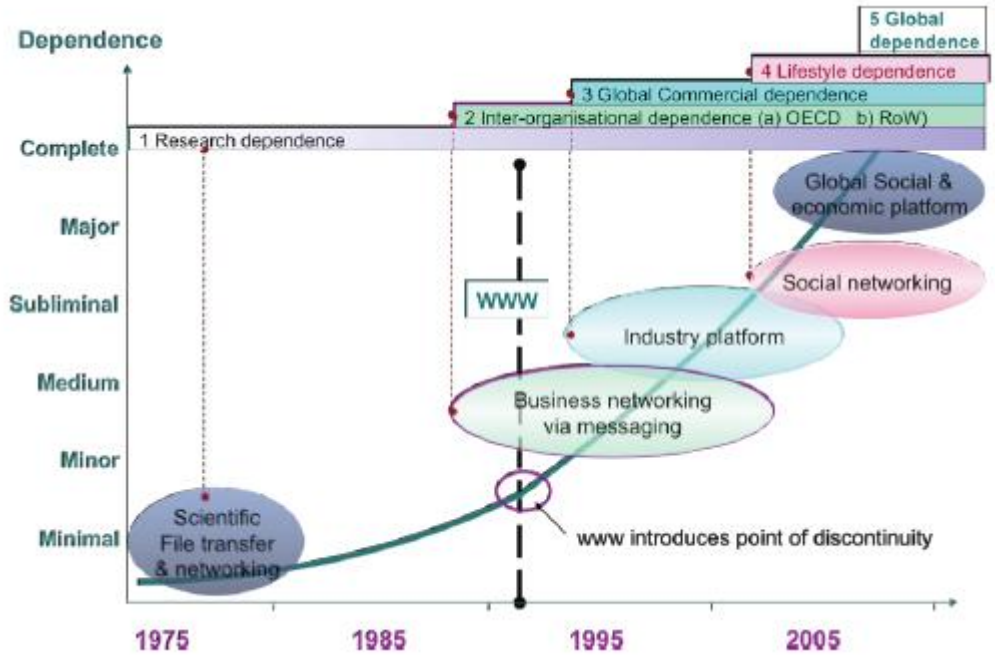
In risk terms the Internet produced: far greater connectivity which provides a vector for criminal activity, considerable opportunity for anonymity, a means by which knowledge of exploitable flaws can be promulgated, and a speeding up of the processes, already noted, by which unsophisticated users can be mislead and exploited,

Figure 1 – Increasing important of the Internet



Source: Towards a Future Internet (2010)

Figure 2 – Increasing dependence on the Internet



Source: Towards a Future Internet (2010)

Future Internet development

The computing and communications technology powering the Internet continues to develop rapidly. Processing power doubles roughly every two years, increasing a million-fold since 1965. Bandwidth and storage capacity are growing even faster, doubling every 12 months. In the medium term, there are no fundamental reasons why these exponential rates of growth should slow down.

The Internet itself is expected to evolve in a more evolutionary fashion. Many more people will connect over mobile access networks, with the next billion users in the developing world more likely to use mobile phones than personal computers. The development of a "semantic" web will allow much greater automated processing of online information. RFID tags and widespread use of sensors and actuators will create an 'Internet of Things' that is integrated into the wider physical environment.

However, fundamental change to the Internet architecture may be difficult given its installed base. Small changes such as the introduction of IP version 6 and multicast have taken a decade longer than expected. Global private IP networks operated by telecommunications companies have more flexibility. Such networks already offer quality of service guarantees, virtual private networks and Voice over IP services. They will soon also offer secure cloud computing services. Google operates its own global private communications network, and other online giants may move in this direction.

On the demand side, the Internet will be a key mechanism for finding and keeping employment, as well being the major social interactive conduit for the majority of people worldwide. Four-fifths of experts surveyed by the EU-funded *Towards a Future Internet* project expected the vast majority of Europeans will find the Internet vital for everyday life in only 5 to 10 years' time.

Most new Internet users in the next decade will live in the developing world and their concerns will become the major drivers for its engineering. This will emphasise a low cost, wireless infrastructure with platforms that can be easily used by billions of individuals with fewer educational resources than are taken for granted in industrialised economies.

Sources: Towards a Future Internet (2010); Anderson and Rainie (2010)

Changing business practices

Enterprise systems in large corporations and governments have seen less dramatic change than in personal computing, but many trends from earlier periods have continued. Older equipment has been replaced by cheaper, faster, more ubiquitous hardware and software. Organisations have become much more dependent on their technology infrastructures. Two developments in particular are worth considering: just-in-time service provision and Supervisory Control and Data Acquisition Systems (SCADA) systems.

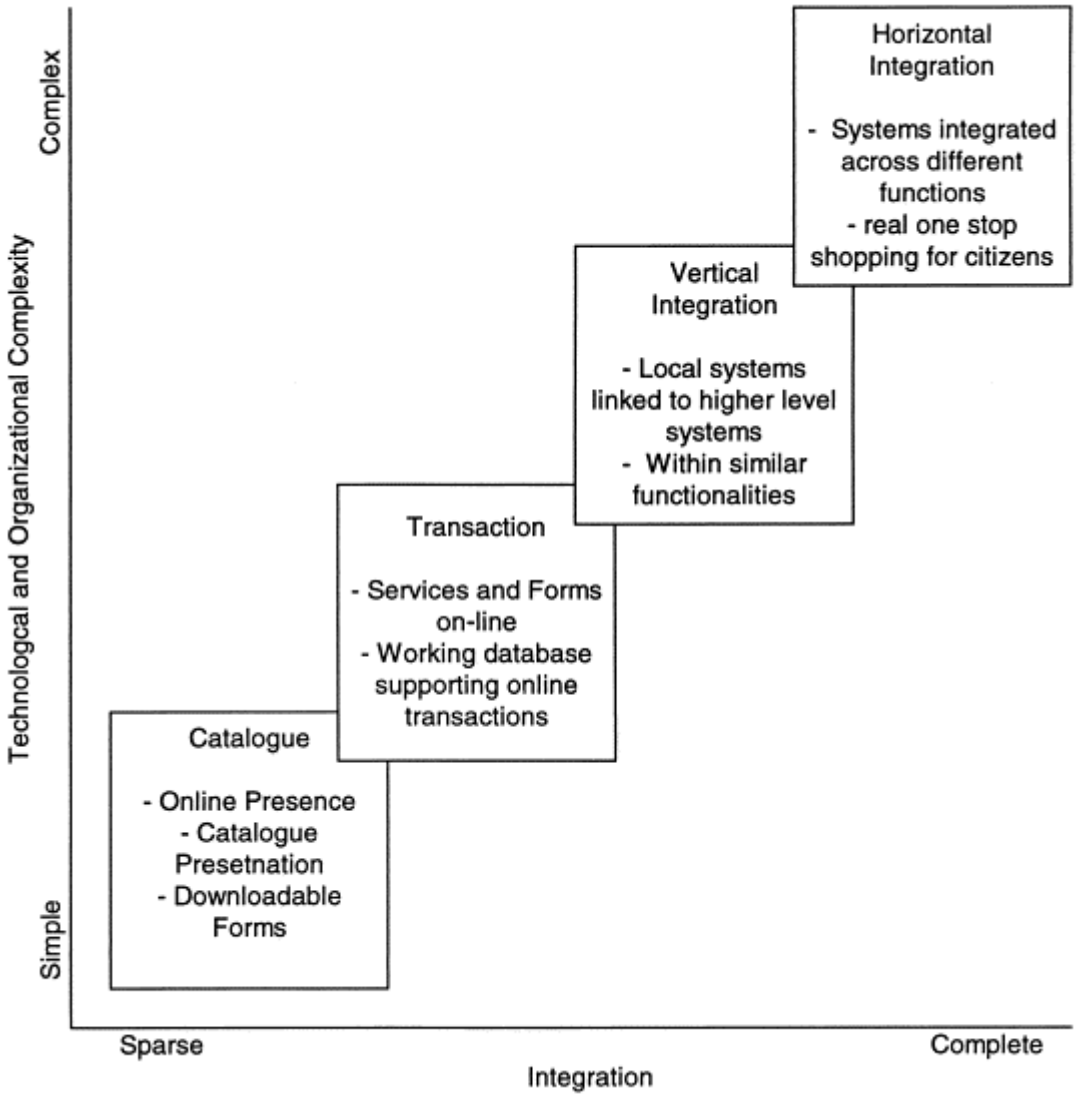
In just-in-time manufacturing, a large company uses its computers to forecast precisely when in the production process it will need materials and components from its suppliers and sub-contractors, and places orders accordingly. This reduces the cost of holding excess stock and makes more efficient use of working capital. Supermarket chains use similar processes in ordering food: computers constantly monitor stock levels, adjust for weather and other seasonal conditions, and place orders at the last possible moment. If computers or telecommunications facilities break down, the manufacturer cannot produce goods and the supermarket will be unable to provide its customers with food.

In the United Kingdom, where nearly 80% of grocery expenditure goes to the 4-5 major supermarkets (DEFRA, 2006), just-in-time methods mean that there is usually 4 days' food supply available on the supermarket shelves at any one time. In 2007 Lord Cameron of Dillington, head of the Countryside Agency, said Britain was 'nine meals away from anarchy.' UK food supply is almost totally dependent on oil (95% of the food we eat is oil-dependent) and if the oil supply to Britain were suddenly cut off Lord Cameron estimated it would take just three full days before law and order broke down (Cameron, 2007). More traditional grocery supply chains still exist in advanced economies, based on local producers offering seasonal food that is purchased from local wholesale markets by independent local retailers. But is considerably diminished as raw food is imported from across the world and processed and packaged in factories. In 2000 consultants Best Foot Forward estimated that Londoners consumed 6.9 million tonnes of food per year, of which 81% came from outside the UK.

E-Government

The general trends towards complexity as they apply in e-government can be seen from the following (Layne & Lee, 2001):

Figure 3: Steps Towards E-Government



Smart Grids and SCADA

The efficient provision of utility services such as electricity, gas, water and oil requires constant monitoring of supply systems. Since the 1960s these systems have been increasingly monitored and controlled using SCADA computing equipment. More recent systems incorporate load forecasting, adjusting the state of a supply network *ahead* of actual demand. Earlier SCADA systems were proprietary to specific vendors, but are now moving to an open networked model. Newer SCADA devices communicate using Internet protocols, sometimes over the public Internet to remove the cost of dedicated communications links. Such systems are much more vulnerable to attack. In July 2010 it became apparent that one widely-deployed SCADA device – manufactured by Siemens – had a hard-coded default password, making it particularly easy to attack. Just such an attack, Stuxnet, appeared shortly thereafter. (Bond, 2010) (Falliere, 2010)

Many systems that deliver essential services and goods have acquired self-organising qualities. Computer programs handle much of the detail of management, with humans setting operational parameters. This self-organisation extends to managing the operations of computers and communications systems, assessing and balancing the demands made on the various sub-systems and where necessary shutting them down when overloaded. The quality of computer self-organisation was predicted as long ago under the name of "cybernetics" by Norbert Wiener (Weiner, 1962) and Stafford Beer in the 1960s and 1970s. This in turn may cause the failure of other interdependent systems.

Cloud Computing

The most significant security-relevant trend in business computing is currently the move to "cloud" infrastructures. Third-party providers are increasingly providing storage and computational resources to their customers, through services such as Google Docs and Gmail and underlying infrastructure such as Amazon 's Elastic Compute Cloud (EC2). The market for these services was estimated at around USD 17 billion in 2009, and is forecast to reach USD 44.2 billion by 2013 (ENISA, 2009: 3).

Cloud infrastructures tend to concentrate data and resources, presenting an attractive target to attackers. They are globally distributed, meaning that confidential data may be held across a number of jurisdictions. However, through replication of systems and more robust and scalable operational security, they may achieve a level of security that would be beyond most smaller-scale enterprises (ENISA, 2009: 4).

Cloud services do face some specific risks, such as the ability of their staff to potentially compromise large quantities of sensitive data. However, providers so far seem to be differentiating their services on security levels (ENISA, 2009: 7—10). With appropriate industry standards and competition between providers, it should be possible for businesses to manage the day-to-day security risks associated with cloud computing. However, less attention so far has been paid to the impact of catastrophic events on cloud services. Without careful resilience planning, customers risk a loss of processing capacity and of essential data.

Complexity / Source Lines of Code / Program Bugs

One irreversible feature of the history of computing has been that operating systems, software applications and the hard-coded intelligence of hardware devices such as motherboards, graphics cards, modems, switches, printers and so on have all become much more complex. One measure of the size of a program is Source Lines of Code (SLOC). In 1993 Microsoft's then top-of-the-range operating system, Windows NT 3.1 had 4.5 million

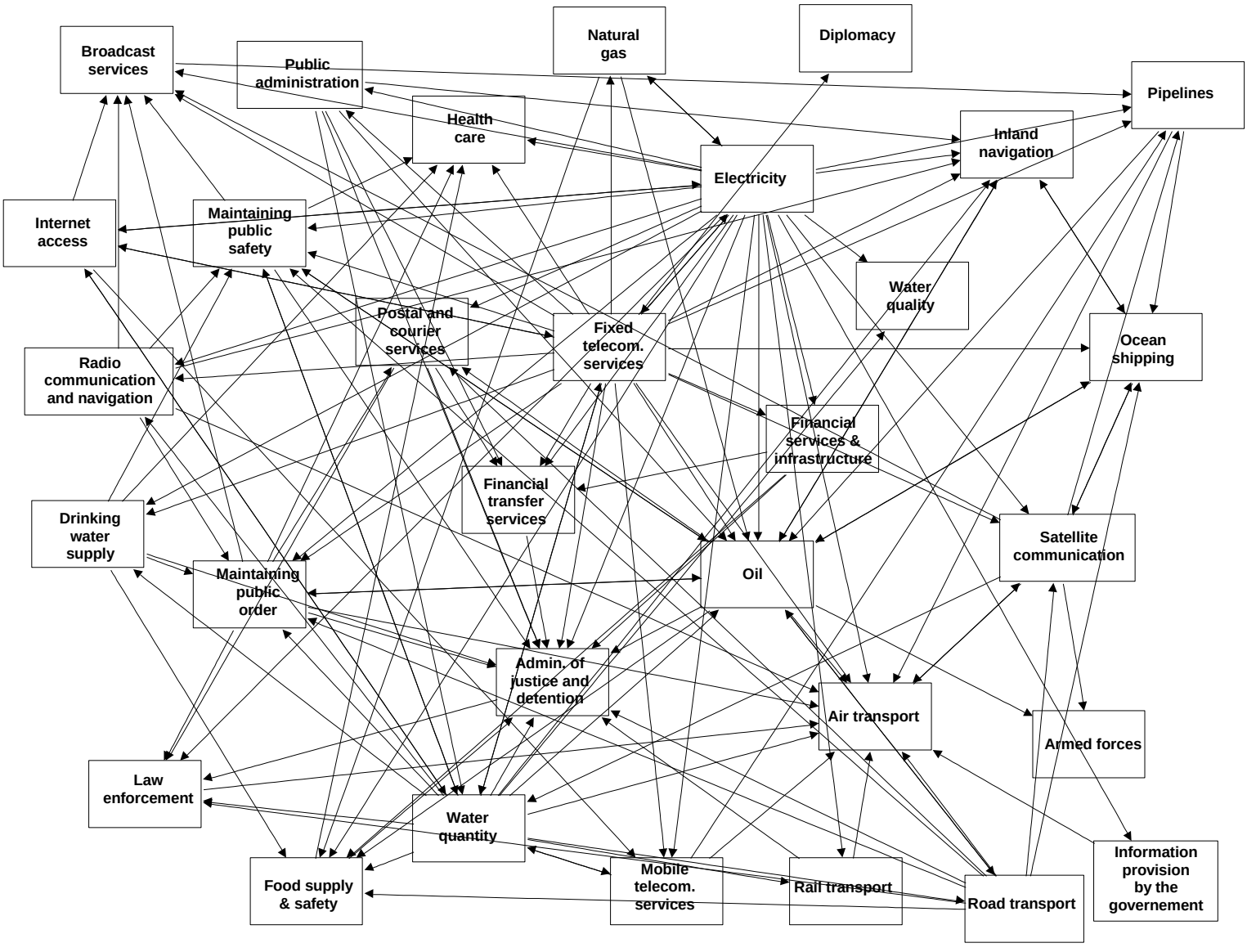
SLOC. Its successor Windows NT 3.5 in 1994 had 7.5 million SLOC. Windows XP, released in 2001 had 40 million SLOC. Figures do not appear to be available for Vista and Windows 7. (Perrin, 2010). This growth in size is not unique to Microsoft but a result of a perceived market demand for new features.

If we assume only one bug or error per 1000 lines we arrive at the possibility of 40,000 bugs in Windows XP. It is this maths, plus the ever-increasing range of inter-actions, that explains why modern operating systems and software are so prone to flaws which, as they become apparent, either cause crashes spontaneously or can be exploited. A further cause for concern is that some software vendors in particular release products in order to secure market advantage and revenue but before they have been fully tested.

Critical Infrastructures: Cyber Elements

The inter-connectedness of various major government services and large private sector systems has lead to the identification of what is referred to as Critical Infrastructures (CI). Government approaches to CI are examined below in greater detail. It is useful to illustrate what is involved: the Dutch TNO produces the following chart of CI interdependencies and stresses the role of cybersecurity in nearly all aspects:

Figure 4: Critical Infrastructure Inter-Dependencies



(Source: Eric Luiff, 2010)

Specific Systemic Threats

This study is concerned with global risks, not those that simply affect individuals and regular commercial and non-profit organisations. However because of the potential for small events to cascade into larger ones, and because the difference between a big event and a small one is not necessarily a matter of technology but of scale, we need a broad overview of the main technology-based threats and associated terminology.

Accidents affecting infrastructure: These can be physical in nature, for example a fire or flood at a critical site; or "logical", which usually means a software failure.

System overload: Information systems are designed to cope with specified levels of capacity and transaction throughput. There will nearly always be a forecast of current and likely future needs and these will be translated into loading factors for IT hardware and software. In abnormal circumstances if resources are insufficient, systems will cease to work, either shutting themselves down in an orderly fashion or going into an error state. Where there are a number of inter-connected systems, a fault or overload in one system that does not close down "gracefully" may result in cascading errors.

Deliberate logical attacks: These are the types of attack that receive most publicity, and include:

Table 1 – Types of Malware

Type	Description
Logic Bomb	The earliest and simplest form of malware was the **logic bomb**, a concealed program that triggered a result that the designers of a system did not expect. The payload could be a jokey on-screen message, complete system shutdown or a complex sequence of events that might result in fraud. Logic bombs probably date back to the 1960s. An early example may have been the Trans-Siberian Pipeline incident of 1982 in which there was undoubtedly a large-scale explosion but also suggestions that computer-controlled equipment had been manipulated. Other examples include an attempt to delete rocket data at General Dynamics in 1992, and actions by programmers at Deutsche Morgan Grenfell in 2000, Medico Health Solutions in 2003, UBS in 2006 and Fannie Mae in 2009.
Trojan Horse	A **Trojan horse** is a program that creates a back-door into a computer. This originally amounted to simply creating a hidden remote access facility. Since the arrival of the Internet, access can be obtained from anywhere on the network. Trojans can be used to monitor the activities of legitimate users, steal or delete data. They can also be used to take over a machine entirely – and then use that machine to hide the real identity of a perpetrator. The taken-over machine, referred to as a **zombie** then becomes a platform for any number of further exploits.
Key-logger	A **keylogger** is a program which monitors and records the keystrokes on a computer; it can be regarded as special form of payload. The usual aim is to capture passwords,
Virus	A **virus** is a self-replicating program that often has a logic bomb or Trojan as a payload. The self-replication means that the perpetrator's success does not depend on immediate access to the target machine.

	Viruses of sorts were deployed in the early 1970s in the mainframe environment but came into their own in the 1980s with the arrival of the PC and the wide usage of floppy disks. The term is said to have been coined in 1984 and in 1986 the first successful vector – the boot sector virus – appeared (Brain). By 1995 ways had been found to hide rogue code in Word documents – the macro virus Concept. Viruses took off in 1999 with the development of techniques to infiltrate emails and email programs (Happy99, Melissa) and to create back-doors (Sub Seven). The ILOVEYOU virus of 2000 is estimated to have caused up to USD 10 million dollars in damages, partly because it was able to spread undetected very quickly.
Root-kit	The term **root-kit** originally referred to a program that took over an entire computer and gave the perpetrator total ("root") privileges. Today it tends to mean a piece of malware that is very well hidden within the operating system of a computer and hence difficult to detect and remove. A root-kit may be the payload of a virus.
Web-based malware	Malware can also be embedded in web pages. Web pages often contain code in languages such as JavaScript. This may be used for such innocent purposes as triggering a moving display or validating the input to an on-screen form. However it can also be exploited to install malware. Another technique is the use of single pixels on a web page which would normally be invisible to the user but which contain a pointer or hyperlink to destructive malware,

A **Denial of Service attack** overwhelms Internet-connected systems and their networks by sending large quantities of network traffic to a specific machine. An attack from a single computer can easily be managed, and so attackers use large numbers of compromised machines to carry out Distributed Denial of Service (DDoS) attacks. Perpetrators must first take over the computers to be used for the attack, typically via email or web-based malware. The attacker operates from a "command and control" computer that issues commands to these compromised machines. Often the immediate "command and control" computer has been compromised and is being remotely controlled from elsewhere.

BotNets

A common enabler of systemic cybersecurity risks is the very large numbers of Internet-connected personal computers that have been compromised by malicious software. These "bots" are connected together into "botnets" of hundreds of thousands or sometimes millions of machines. Two recent examples are the Conficker network of 7 million machines and the Spanish-based Mariposa network of 12.7 million machines. (McMillan, 2010)

Bots are globally distributed. In 2006/2007 the Honeynet Project found the highest number in Brazil, followed by China, Malaysia, Taiwan, Korea and Mexico. The command-and-control servers directing these machines were mainly found in the US, then China, Korea, Germany and the Netherlands. (Zhuge et al., 2007). Botnets are available for rent in criminal markets, for as little as USD 0.04 per bot – with support services included (House of Lords EU Committee, 2010: 155). They are an infrastructure for attacks that provide bandwidth, enable the circumvention of network restrictions and mask the location of attackers: "the ultimate source of such attacks can seldom be attributed with any confidence to a particular country, let alone a particular individual" (House of Lords EU Committee, 2010: 9).

Zero-Day Exploits / Attacks

A zero-day exploit is one that uses a hitherto unknown technical vulnerability for its effect. Most exploits emerge relatively gradually, from experiments or papers by researchers, and then spread slowly through networks and computers. In these circumstances it is usually possible for the vendors of security technologies such as virus scanners, firewalls and intrusion detection scanners to identify and block malware before exploits cause real harm. This is why many virus scanners can detect several thousand viruses while much smaller number are active "in the wild". In the zero-day situation, the exploit is already in wide distribution before detective and preventative means have been developed.

During 2009 Symantec documented 12 such vulnerabilities. Four were in Adobe's PDF Reader software, while six were in Microsoft software such as Office and Internet Information Server. These vulnerabilities were exploited in both generic phishing attacks and by malicious code that appeared to be targeted at high-ranking business executives (Symantec, 2010: 45). Just one zero-day vulnerability in Internet Explorer was used to breach systems at Google, Adobe and a number of other high-technology firms (Zetter, 2010).

Embedded Malware

Very large numbers of everyday objects now include miniature, limited function computers. The same is true of many machines used in industrial processes, in telecommunications equipment and in weapons systems. In some instances the processing capability is quite limited, but in others versions of operating systems familiar to PC owners are used. Embedded versions of Windows XP are deployed in banking ATMs and some transportation ticketing systems. Versions of Linux appear in Internet routers and media players. Whereas traditional software versions of operating systems and programs are easily modified during the routine use of PCs, embedded system software is usually more difficult to update. On the other hand the original manufacturers and specialist repair staff can insert malicious software that accepts additional covert commands. In an article for *Foreign Affairs* General Wesley Clark and Peter Levin reported that a 3-kiloton explosion in a Siberian gas pipeline in 1982 was the result of CIA activity in embedding faulty chips into equipment that had been purchased by the Russians. They also mentioned the possibility that an Israeli raid on Syrian nuclear sites in 2007 was made easier because of embedded malware that turned off Syrian defence radar (Clark and Levin, 2009). In 2009 the Indian government became concerned about the possibility of embedded malware in telecommunications equipment manufactured by the Chinese company Huwaei (SpamFighter, 2009).

Whereas malware deployed on regular personal computers is relatively easy to detect, testing embedded systems, particularly when the tester does not know what a "clean" system should look like, presents significant challenges.

Deliberate physical attacks: The extensive interest in logical attacks can divert attention from attacks that are largely physical in nature. In many respects the use of bombs, direct tampering with computer hardware and the severing of cable connections are both easier to achieve and more likely to have lasting effects, since replacements for damaged equipment must be sourced and installed.

There is a long tradition of dissident groups targeting computers. In 1969 a group of peace activists called Beaver 55 destroyed 1000 data tapes using magnets. Between 1979 and 1983 a French group called CLODO destroyed a number of computers in Toulouse (Wong, 1983; Cornwall, 1987). The Unabomber (Theodore Kaczynski) carried out 16 bombings in the mid-1990s. None of these events caused much collateral damage, still less a cascade. However, societal dependency on computers and communications systems and the inter-connectedness of critical systems has increased substantially since. After the 1993 IRA bomb attack in the City of London, Lloyds paid out over GBP 350 million in insurance losses and almost collapsed

(Coaffe, 2003). The World Trade Center bombing of the same year hit many computer dependent companies; 40% of these companies were bankrupt within two years.

Significant problems can be caused if cables carrying Internet and other communications traffic are severed. In January 2008 and later the same year in December, the severing of two cables, FLAG Europe Asia and SEA-ME-WE-4, knocked out connections to much of the Middle East and parts of South Asia (though Saudi Arabia was less affected because of its use of satellites) (Singel, 2008).

An **electro-magnetic pulse** (EMP) is a burst of high-energy radiation sufficiently strong to create a powerful voltage surge that would destroy significant number of computer chips, rendering the machines dependent on them useless. It is one of the few forms of remote cyber attack that causes direct permanent damage. The best-known trigger for EMP is with a high-latitude nuclear explosion and was first noticed in detail in 1962 during the Starfish Prime nuclear tests in the Pacific. Studies have investigated the possible effects on the United States power grid. (Oak Ridge National Laboratory, 2010).

Attempts have been made to develop non-nuclear methods of creating EMPs, such as High Energy Radio Frequency (HERF) guns. There are a number of practical problems in turning the phenomenon of EMP into a practical, deployable weapon. First, any such "gun" depends on the rapid release of large quantities of energy that must first be stored and then released very rapidly in a manner that does not destroy the "gun" and anyone close by. Second, a means has to be found to focus and direct the energy so that the aggressor's own computer equipment is not affected. Third, the actual impact may be difficult to forecast. Computer chips within a properly shielded and earthed cabinet may survive. Radio equipment, which needs antennas to function, is much more vulnerable. (Crabbyolbastard, 2010).

In June 1996 the London *Sunday Times* reported that HERF guns had been used to extort GBP 400 million from City of London financial firms. However the story has been consistently and robustly denied and it is surprising that there was never any evidence of collateral damage, for example to traffic lights, even if all the alleged victims had conspired in a cover up.

Solar Flares are large bursts of energy from the sun. Peaks of activity occur every 11 years. They produce radiation across the electro-magnetic spectrum. Some radio transmission – high frequency or short-wave radio – is enhanced but the main effect on satellite and radar is interference. Exceptionally high levels of burst could burn out some electronic components including some of those in satellites and communications grids. Much of Quebec's electricity supply was knocked out during a storm in 1989. The last major event was in 1859. The units at greatest threat are those that have long cables or other devices which act as antennae to draw the power burst into the vulnerable components. However experts disagree about the actual levels of flare required to cause significant damage to modern components and the frequency with which such flares might occur. (Dyer, 2010 and Owen, 2010) The next sun-spot peak is expected in 2012-2013.

What makes a cyberweapon?

There is an important distinction between something that causes unpleasant or even deadly effects and a weapon. A weapon is "directed force" – its release can be controlled, there is a reasonable forecast of the effects it will have, and it will not damage the user, his friends or innocent third parties.

In evaluating any specific cyberweapon, the questions therefore are:

- Is this something whose targeting and impact can be controlled (is there a risk of friendly fire?)
- What success rate can be expected in terms of targets?
- Is there any collateral damage?
- What resources and skills are required?
- How much inside knowledge and/or inside access of target is required? How easy is this to achieve?
- Can the weapon be detected before or during deployment?
- Can a perpetrator be detected during or after deployment?
- What are the actual effects and how long do they last?
- How long can an attack be carried out before it is thwarted by counter-technology?
- How long can an attack be carried out before perpetrators are identified?

For those attempting to assess whether a cyberweapon may be used against them, there is a further question: in terms of likely perpetrators, how well does this fit in with their world-view and stated aims?

On this basis it will be seen that the most common forms of virus on the one hand and the EMP bomb on the other, fail as credible cyberweapons, because they are relatively difficult to control. However a targeted DDoS is a likely cyberweapon.

The range of cyberweapons gives an aggressor more flexibility. Low-level cyberweapons such as website defacements and psy-op related spam can be important in conditioning and persuading the public. Slightly high-level attacks such as a short-term denial of service can do the same job as "going on exercises" and brief "accidental" territorial intrusion.

One advantage that cyberweaponry has over kinetic weaponry is that it is much easier to create ambiguity about who is mounting the attack – the "attribution" issue.

A further advantage is very low cost. A single individual can mount a DDoS attack using a single personal computer. All of the effort is expended by computers owned by others and which have been taken over as part of a botnet.

Attribution of Cyberattacks

Most cyberattacks are mounted from computers that have been taken over and are remotely controlled not by their owners but by third parties; often the actual owners are unaware of what is happening. The basic tool of the Internet detective is *netstat* which provides the IP address of the attacking computer. Thereafter the detective must obtain the name of the owner, which will usually involve approaching an Internet Service Provider – this task is much more difficult if the detective is one country and the ISP is in another jurisdiction. Rotenberg, 2010, describes some of the legal obstacles but he concentrates on privacy and human rights whereas there may also be issues in mutual legal assistance treaties. Once access to the attacking computer has been obtained it has to be examined for the presence of its command-and-control software; this should point to the remote controlling computer, but it may simply identify another computer which is itself being remotely controlled. Attribution therefore is always difficult and takes time, too long for swift retaliation. This feature gives suspected attackers a significant layer of deniability. Allegations of attacks by, for example Chinese or Russian government-sponsored entities can be countered by the suggestion that Chinese or Russian computers had simply been taken over by perpetrators from a third country or were the actions of "patriotic hackers" (Hunker, Hutchinson, Margulies, 2008)

Blended attacks

A blended or combination attack is when a conventional "kinetic" attack is accompanied by a logical attack with the purpose of disorientating victims. In principle this is not new – in kinetic war a routine tactic is to disrupt the radio communications of the enemy by jamming radios and/or creating misleading radio traffic.

In today's network-enabled wars the disruption has to be to networks as opposed to radio nets. Operations of the United States and its allies in Kuwait in 1990-91 and Iraq in 2003 were both accompanied by "electronic warfare". During the Georgia/South Ossetia conflict of 2008 there were widespread disruptions of Internet traffic in the region (Shachtman, 2008). There have also been allegations of Hamas-linked cyber-attacks on Israel in 2008 (Home Security Newswire, 2009).

Large-scale criminal attacks

Transactions and payments are increasingly made online, with 70% of younger UK Internet users banking online and two-thirds of all adults purchasing items online (UK Payments Council, 2010: 20). Fraudsters have unsurprisingly adapted techniques to dip into these new financial flows. Rather than attack the well-protected internal systems of financial services institutions, they commonly use malicious software to infect personal computers and steal passwords and personal information that allows theft from online bank accounts. Users are also misdirected to fraudulent websites (often hosted on botnets) that impersonate banks and acquire account details and passwords (so-called "phishing").

Money can be moved out accounts via dupes known as "money mules" that make it harder for the destination of funds to be identified. Fraudsters also use stolen personal information to apply for and exhaust credit cards and loans, leaving impersonated individuals to clear up their damaged credit histories and banks to carry these losses (Brown, Edwards and Marsden, 2009).

Financial services institutions have so far been able to manage this fraud, absorbing losses suffered by consumers while requiring merchants to carry the risk of many "card not present" remote payments. Losses are significant (with online banking fraud totalling GBP 59.7 million in 2009 in the United Kingdom, where the most detailed data is gathered), but in relative terms remain low, with Visa Europe reporting their overall annualised fraud rate declining to 0.06% in the year to June 2009 (Visa Europe, 2009: 30). Herley and Florencio estimated total phishing losses in the United States at USD 61m in the 12 months to August 2007 (2008: 9). Even wider measures of online fraud against businesses remain low: "a long-standing annual survey of large organizations reveals that accounted-for costs have only recently exceeded USD 1 billion dollars" (Libicki, 2009: 37).

However, there is a growing criminal industry that produces and supports malicious software, and global connectivity between criminals and victims created by the Internet. This is reducing the marginal cost and increasing the benefits and supply of crime (van Eeten and Bauer, 2008: 16). Herley and Florencio tentatively calculated that the market entry and behaviour of "phishermen" was rational, and that low barriers to entry has resulted in phishing becoming "a low-skill low-reward" business. They go on to say: "Repetition of questionable survey results and unsubstantiated anecdotes makes things worse by ensuring a steady supply of new entrants" (2008: 1).

Management of fraud by banks and payment providers, while welcome to consumers, reduces incentives for lowering the systemic risk of widespread PC insecurity. A risk remains that more successful criminal activity will "tip" these conditions into a systemic consumer distrust in online banking and payment systems, lead to unacceptable costs of fraud for businesses, as well as providing an increased funding stream for other criminal activities.

The typical cyber-extortion involves the use of botnets to deliver a denial-of-service attack which is then followed up by an offer of "consultancy services" to remove the problem. In 2005 three Dutchmen were arrested in connection with a scheme in which hundreds of thousands of computers were allegedly infected with malicious computer code (Brandt, 2005). In the previous year botnets were used in attacks on a number of gambling sites (Berinato, 2006). Joseph Menn has documented the use of botnets against a number of online gambling sites. He discovered the involvement of the US mafia, criminal gangs operating out of St Petersburg, and a rogue Internet Service Provider that at one stage provided hosting facilities for a number of criminal activities including the distribution of sexually indecent images of children (Menn, 2010).

Recreational Hacking

Recreational hacking is the type of activity that appeared in the 1983 movie *War Games.* The aim is usually to impress other hackers with a skilful exploit rather than to make money (Cornwall, 1985). The problem is that such recreational activity can have unintended consequences and become a global risk. Examples include:

- The Morris worm of 1988, written by a student as an experiment, but which went on to infect many major Unix computers on the nascent Internet.
- In 1994 United Kingdom-based hackers Datastream Cowboy and Kuji attacked computers owned by the United States Air Force, NATO, NASA, Lockheed Martin and others (GAO, 1996; Sommer, 1998).
- The Melissa virus of 1999 created by David Smith is estimated to have spread to over 1 million PCs world-wide causing damage up to USD 400 million. It could be embedded in documents created in the popular Word 97 and Word 2000 formats but could also mass e-mail itself using Microsoft Outlook (F-Secure, 2006).

- Mafiaboy, a 15-year-old Canadian, is alleged to have successfully attacked some of the largest commercial websites in the world, including Amazon, Ebay and Yahoo, in early 2000 (Evans, 2001).

Hactivism

Hactivism is the use of hacker techniques such as web-defacement and distributed denial of service to publicise an ideological cause rather than for crime (metac0m, 2003) The earliest examples predate the public Internet: in 1989 the United States Department of Energy and NASA Vax VMS machines were penetrated by a group called Worms Against Nuclear Killers (WANK) (Assange, 2006). Significant examples include UrBaN Ka0s who in 1997 conducted a campaign against the Indonesian government, Electronic Disturbance Theater who disrupted Republican websites during its National Convention in 2004, campaigned against the right-wing Minutemen movement in 2006 and against cuts to Medicaid in 2007, and the so-far-unidentified group that attacked the Climate Research Group of the University of East Anglia and posted selected stolen emails which they claimed showed bad faith and bad science in relation to the global warming debate.

In 2009 during the Israeli invasion of Gaza, web-site defacements, domain name and account hijacks and denial of service attacks appear to have been carried out by supporters of both Israel and the Palestinians, (Graham, 2009).

A group called Anonymous appears to have had a number of campaigns, in favour of Iranian dissidents, against the Church of Scientology, against music and film industry bodies and lawyers seeking to punish downloaders of copyright material, against the Australian government's plans to filter the Internet and, most prominently, in 2010, against companies such as Mastercard, Visa and PayPal who had withdrawn supportive payment facilities to the Wikileaks site (Ernesto, 2010and Halliday and Arthur, 2010).

The main practical limitations to hacktivism are that the longer the attack persists the more likely it is that counter-measures are developed and put in place, perpetrators identified, and groups penetrated by law enforcement investigators.

Hacktivism is a first cousin to more conventional direct action groups, which all face the same challenge: the initial actions are often successful in winning public sympathy but thereafter public perceptions can arise that activities have "gone too far". Because nearly all hacktivists use anonymising technologies it is not always easy to distinguish their activities from covert cyber-attacks carried out by government agencies (Hunker, Hutchinson, Margulies, 2008; House of Lords European Union Committee, 2010).

To reach the level of a global shock hacktivist activity would need to be extremely well researched and persistent and be carried out by activists who had no care for the consequences. In the case of the 2010 Anonymous attacks on financial services successful prolonged and ever-changing denial of service attacks might have "gone global" as large numbers of companies dependent on credit card facilities to collect funds would have gone out of business, triggering unemployment among their staff and perhaps triggering further financial failures among their suppliers. One can also envisage an unintended global shock arising from attempts by ecology-minded campaigners using DDoS techniques against some industrial or communications component which they regarded as symbolic of a lack of care for the future of the world's ecology but where the effect was to trigger a cascade of network failures resulting in wide-spread loss of essential supplies of power and which in turn caused extensive economic loss.

Large-scale State and Industrial espionage

There is nothing new about industrial espionage or state-sponsored industrial espionage. In 1981 a substantial cache of 4000 documents was provided to the French intelligence service by Col Vladimir Vetrov (Agent Farewell). They showed a highly organised Soviet KGB "science and technology" orientated espionage operation, later analysed and explained by the CIA (Weiss, 1996). In 1994 Michael John Smith was convicted at the Old Bailey in London of spying on the United Kingdom's science and technology activities for the KGB (Cryptome, 2006). These activities have simply moved into cyberspace.

A highly detailed account of cyber-espionage in 2009 and 2010 can be seen into two reports from Canadian researchers. The first deals with Chinese attempts to track the activities of the Tibetan government-in-exile of the Dalai Lama and its sympathisers by the use of remotely controlled malware. The researchers claim to have found at least 1,295 infected computers in 103 countries (Information Warfare Monitor, 2009). The second report contains a great deal of information about highly organised Chinese targeting of, among others, Indian government computers (Information Warfare Monitor, 2010).

The aims of industrial espionage specifically include saving money on research and development, undercutting a rival's competitive tender, and carrying out a spoiler exercise to a marketing campaign The effects of successful industrial espionage may be very significant for a single corporate victim. In the longer term they may also significantly affect national competitiveness. A former CIA clandestine services operative turned commercial security advisor in 2008 provided a useful review of recent activity against Germany, Japan, Taiwan, Australia, New Zealand, Canada, UK, France, the Czech Republic, Qatar, South Korea and the United States. (Burgess, 2008)

A great deal of effective espionage can be conducted without the need for sophisticated technology. The requirement for information comes first and the technical methods used are secondary. In the 1970s and 1980s the pre-occupation in technology terms was with micro-radio transmitters or "bugs". Non-technical methods include:

- Collection and analysis of open source material (competitor intelligence). The web and social networking sites have made the task of the desk-bound investigator much easier and more rewarding.
- Targeting of specific individuals to probe for weaknesses in their use of physical security or opportunities for blackmail.
- Subversion of employees, perhaps in the context of a new job offer.
- Infiltration of fake employees.
- Use of third parties such as journalists and consultants, advertising agents and printers.
- The examination of waste material

It should be noted that most technical methods also require a great deal of research about targeting of individuals and ICT equipment if they are to be successful. Clumsy research may lead to the premature identification of the espionage attempt. Some writers and marketeers use the phrase "Advanced Persistent Threat" to characterise series of actions involving sophisticated technical and clandestine means to collect intelligence about targeted individuals and organisations. (Sterling, 2010)

Cyberespionage has the potential to cause significant financial loss to victims; it may also impact on the security of nation states both militarily and economically. However it is difficult to envisage a scenario which meets a "global shock" test.

Remedies

We now turn to the techniques and doctrines of information system security as these provide the main means by which an "event" can be prevented or at least managed. A "doctrine" is a philosophical approach. Other remedies concentrate on how a system is designed. There are a number of problem-specific technologies. Finally we look at what happens when these have failed, a security "event" has taken occurred, the effects must be mitigated, and recovery somehow achieved.

Remedies: Security Doctrines

As systems and their usage have become more complex, security doctrines have had to evolve.

The earliest doctrine was "**technological problem/technological solution**". Any problem associated with technology was viewed in purely technical terms and it was assumed that there was some technical solution. Thus: unauthorised usage of a computer is to be addressed by an access control facility, and viruses can be eliminated by the use of virus scanners. This doctrine still applies in some measure, but as a total response is quite inadequate.

In the late 1960s increasing use was made of **audit**, which was designed to spot control deficiencies in systems. Electronic Data Processing (EDP) auditing borrowed extensively from regular accountancy-type audit. Audit, however, needs to be carried out against a standard that indicates what is "good" or "acceptable". This can point to the main deficiencies in EDP Audit: who determines the content of these standards? Is there adequate machinery to cope with the very rapid change in technology and how it is deployed? Is it easy to acquire an apparently valid audit certificate of compliance with a "standard" but which does not reflect current usage and risks? **Security Standards** are still popular in some circles today, though more modern standards such as ISO27000 tend to focus more on the process of analysing risk rather than simply having a long list of elements to be checked off.

In the 1990s there was a shift towards concepts of **risk management** using ideas developed earlier in the insurance industry. Risks can be identified, analysed and prioritised. A risk manager can decide to avoid a risk by means of not carrying out that particular type of activity, reduce risks also by the use of technical measures, contract a risk away by taking out insurance, or accept a risk, because the costs of any alternative route is too high. Risk management techniques are also used to control market risk, credit risk and operational risk.

Risk management approaches are most useful when there is a reasonable level of available reliable data about the risks being considered – where there are probabilities and clearly definable potential financial losses. In the regular insurance domain, for example, there is actuarial data about the likelihoods of motor accidents, fire occurrences and length of human life. The extent of an insurer's liability is defined by the insurance contract. However technology-related risks are much more difficult to assess because the rate of change is such that no actuarial data can be built up. There are also problems when calculations have to be made about intangible losses, such as losses of reputation and goodwill.

Within the national civil contingencies agenda, potential losses are even less tangible – how do you calculate the dangers of community breakdown, for example? The response usually is to adopt a three level matrix of high, medium and low levels of probability, and another three level matrix of impact, which allows for some of the disciplines of risk management to be adopted without the need for precise financial calculations. (Cashell, 2004)

Towards the end of the 1990s, analysts began to use the phrase **information assurance**. This is an altogether "softer" form of analysis, which recognises that in the absence of solid risk data it is better to identify all the elements that make it more or less likely that there will

be a security breach. The approach retains many elements of risk analysis and does not altogether dismiss the virtues of security standards, but it also seeks to borrow ideas from the social sciences: management science to understand how organisations work and how security considerations operate within them; anthropology and criminology to identify how individuals and groups behave and are motivated; psychology to develop an understanding of "people" factors in the design of ICT and security; and economics to understand how organisations make security decisions (Backhouse and Dhillon, 2000).

Remedies: System Design

Systemic/Design/Security Requirements

This approach integrates security features into the initial "requirements engineering". A great deal of effort is expended on determining with the customer what system functions are required, including security. Although this is will result in a reasonably secure system, it is often unattractive to the advocates of a new system. The process of identifying requirements can result in delay and apparent additional cost. However, adding security features after the event is often both unsatisfactory and costly. OECD has issued '*Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security'* (OECD, 2002).

Fail-safe

In addition to anticipating likely security breaches, there is a further requirement that whatever happens, fail-safe systems can shut down in a safe mode. The approach is typically used for intrinsically dangerous situations, such as the management of nuclear power stations and robot assembly lines. Usually fail-safe systems are very stripped down, minimising complex interfaces and functions that could be the source of programming errors. (Mukhopadhyaya, 1992) (Pham & Galyean, (1992).

One hazard of fail-safe design is that when one part of a larger system closes itself down gracefully, its traffic gets passed on to another machine that then closes itself down to avoid being overloaded. This can then lead to a classic cascade effect as seen in the 1993 power outage in the north-east United States and Canada. Fail-safe systems need very careful analysis at the specification stage.

Remedies: Detective and Preventative

Specific Security Technologies

These are the main classes of protective technologies available. In terms of "global shock" – a failure adequately to protect a sensitive system could give a hostile complete control over it and also the means to masquerade as a legitimate user. The opportunity to breach basic routine security often provides the first essential step in the more complex series of actions necessary to achieve an event of global significance

Information Security Technologies	
Access Control and Identity Management	The username/password combination has been a fundamental of computer access control since the early 1960s. The main problems are of management – how to securely issue passwords; how to handle individuals who are no longer authorised to use a system, or whose changed role means they need different types of access? As the number of users increase, so the sophistication of the system needs developing. But more is demanded of the user as a result – this may be beyond the capabilities of the less technophile sections of the population. Systems may require different passwords for different services. Identity tokens and two-factor authentication rely on the underlying soundness of the physical artefacts and on careful "human interface" engineering.
Authentication	In addition to the need to authenticate users on a particular system there are wider requirements to link individuals to their various digital identities so that they can be shared across several different environments. Documents need to be authenticated as having originated from a trusted source and that they have not been subsequently altered. The main technical method for achieving this is using digital signatures implemented within a PKI – a Public Key Infrastructure (see also cryptography, below)
Malware scanners	Software that regularly scans files and messages for malicious code. Can also run on a hardware appliance through which all communications traffic is routed. A further option is to route all an organisation's data traffic through the facilities of a specialist vendor. The software carries a large database of the signatures of known viruses, Trojans and other malware; the database is usually updated daily. The main concern is the so-called zero-day exploit – malware that is able to spread undetected for some time before vendors become aware of it and are able to identify a signature.
Firewalls	A program or item of hardware that limits access to a computer across a network, including the Internet. A firewall program will monitor traffic both into and out of a computer and alert the user to apparent unauthorised usage. As with malware it relies on frequently updated signatures. The absence of a firewall makes it much easier for a computer to become part of a botnet and hence cause damage to other computers

Information Security Technologies	
Intrusion Detection Systems (IDS)	An IDS looks for activities that might be associated with unwanted intrusions rather than claiming to detect the intruder directly. The intent is to identify the steps leading up to an intrusion rather than wait for the intrusion to take place. As with malware, the process consists of testing against a series of signatures of "unwanted" events. Many successful intrusions are preceded by a number of investigatory probes and it is these that the IDS identifies. The main practical problem is setting an appropriate alert threshold – in much the same way as a burglar alarm may be too sensitive to passing traffic or not sensitive enough when someone is actually breaking in. Too great a sensitivity leads to many false positives, an inadequately set system results in false negatives – the IDS reports that all is well, when in fact it is not.
Cryptography	Cryptography is used in two main ways in information security. The better known is to provide confidentiality by encrypting stored data and data in transit. The classic management problem in cryptography, apart for the need to determine that the underlying mechanism is sound and not easily broken, is key management. How do you pass on the keys needed to decrypt data in a secure fashion? The larger the population of people who need to be able to share encrypted information, the greater the problem. The solution is via public key cryptography where, because different keys are used to decrypt and encrypt and a pair of keys is required, one key can actually be published. The discovery of public key cryptography also made possible the development of systems for authentication and safe identification of documents, machines and individuals.
Load Balancing	The aim of load balancing is to distribute workload among several computers, and to be able to do so dynamically. In normal use the aim is simply to optimise available computer resources. A common application is to be able to offer what appears to be a single service (for example a very large website) from several actual machines. But the technique can also be used in a security context, particularly where a website and associated services may come under a DDoS attack. Load balancing is also used in telecommunications services, to cope with physical loss of a cable or switching centre,.

Information Security Technologies	
Penetration Testing	Modern information systems are so complex and so prone to rapid change that even in those situations where a great deal of trouble has been taken to analyse risks and put in place appropriate remedies, there are still likely to be security holes. Hence the use of so called ethical or white-hat hackers – specialists who run through a repertoire of intrusion techniques to probe for weaknesses. The tools used are carefully researched and constantly updated as new weaknesses become publicised (Orrey, 2009). They are also heavily automated. Penetration testers operate within a strict framework of "rules of engagement" to ensure that there are no untoward side effects. Many governments have testers on their permanent staff and in addition employ from the commercial sector. Vetting is essential; in the UK it is carried out for government purposes either by one of the security and intelligence agencies, the police or the Defence Vetting Agency.

Remedies: Mitigation and Recovery

When preventative and detective methods fail – the emphasis switches to mitigation and recovery.

Figure 5 – Shape of Disaster Recovery

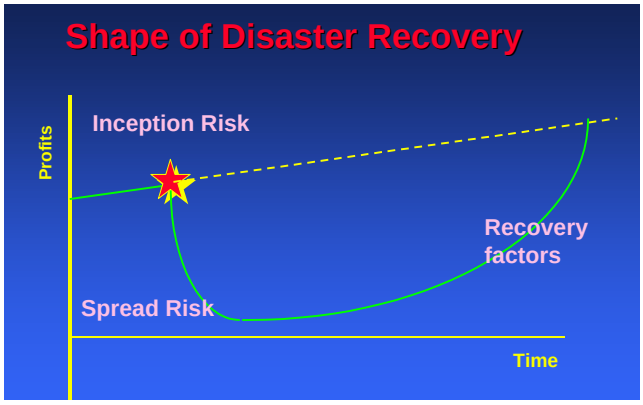


Figure 5 shows a relatively simple type of disaster, without side or cascade effects. Several things should be noted: the y-axis is marked "Profits" but for a non-profit or government services organisation it could equally refer to "throughput" or "transactions". Second, "Inception Risk" and "Spread Risk" are unconnected – the first refers to vulnerability or exposure to hazards, the second is the impact of an event once it has occurred and is a function of the structure of organisation that is affected. "Recovery Factors" also are a function of the structure of organisation that is affected but also whether, among other things, there is a well-tested contingency plan.

The aims of a security plan are to:

- Reduce the probability that a triggering event takes place by having in place good preventative and detective measures;
- Limit spread by careful analysis at the point of design and by having in place mitigation measures;
- Reduce the time taken in recovery by having a well worked-out and tested set of contingency plans.

The most complete form of contingency planning requires an organisation to have a duplicate infrastructure of computers and communications networks with continually updated data. Such a plan also requires the instant availability of alternative premises and arrangements to move staff. Few organisations can justify the costs of such a plan. and calculations have to be made about how long it can afford to be offline and which elements of its overall operations ought to be given priority in any recovery. The design of such a plan requires a careful business analysis as well decisions about appropriate levels of associated investment. A characteristic of nearly all recoveries is the need to cope with enquiries about how the recovery is proceeding – the longer the recovery takes the greater the level of "enquiry" traffic. See, for example, http://www.ibisassoc.co.uk/contingency-planning.htm and http://www.bcpgenerator.com/ for commercial approaches.

Any plan needs frequent testing and updating if it is to be viable in a real emergency. Some aspects of contingency planning can be contracted out, including the detailed design of a plan and the maintenance of stand-by equipment and premises. For large and complex organisations there are fewer options for such specialist third-party services.

Although the failure of a computer system may be the trigger for a "disaster" or may have a multiplier effect, computing and communication systems are also a key mechanism for catastrophe mitigation and post-event recovery:

- If nearly all of an organisation's records are in digital form, they can be readily and frequently backed-up and stored remotely much more easily than paper-based records.
- Essential computer systems can be duplicated off-site. Although some organisations have their own dedicated disaster recovery facilities, there are also a number of specialist companies that offer services such as stand-by computers, emergency sites and skilled technical staff.
- Given enough pre-planning, organisational communications infrastructures can be rerouted and redirected to alternate sites.
- To a limited extent systems can be designed to self-organise repairs if one component is damaged – this happens most frequently with telecommunications services and is of the essence of the reason why the predecessor to the Internet was developed
- Computers can also be used to maintain, support and execute a recovery program – including the storage of detailed lists of necessary actions, essential contacts and copies of critical operational documents.

Risk characterisation, interlinkages and knock-on effects

One of the difficulties in promoting a sober public assessment of cybersecurity threats is the plethora of articles and news-features which extrapolate speculatively from the uncovering of program or operating system flaws, or from the news that an item of malware uses a hitherto unknown technique and has been found in the wild.

In seeking to identify scenarios with potential global effect, we need to consider the notions of "tipping point" and "cascade".

The basic concept of cascade effects can be illustrated using recent events. An oil spill in the Gulf of Mexico results not only in the loss of oil, but potentially long-term damage to relatively poor parts of the United States relying on tourism, fishing and the supply of seafood to shops and restaurants throughout the US. Icelandic volcanic ash over Europe closed air space, allegedly causing over USD 1 billion of losses to airlines and massively inconveniencing tourists and business people, many of whom were delayed from returning to work. Some 100, 000 flights were cancelled and 7 million passengers stranded (Volk, 2010).

Most systems are designed for expected normal levels of activity, with an allowance for expected growth and a further allowance to cope with "unexpected" demand. However in a catastrophe they can reach a tipping point once the design specifications are exceeded. The system can become overloaded and cease to function at all. Load may then be passed to another similar system, which is put at risk of collapse. Other systems may rely for their functioning on receiving information from the first system (Peters, Buzna and Helbing, 2008; Rudolph and Repenning, 2002). Some network designs may be vulnerable to a large-scale cascade triggered by the disabling of a single key node (Motter and Ying-Cheng, 2002). In resilience planning it is important to identify such tipping points and anticipate accordingly.

Hines and others have investigated the extent to which topological graph models are useful for modeling vulnerability and tipping points in electricity infrastructure. They concluded that many existing theoretical models give misleading results. (Hines, Cotilla-Sanchez, Blumsack, 2010).

Industry structure can have a significant impact on the systemic consequences of system failure. Borg (2005) identified three key structural features:

- Redundancies: systems can substitute for other systems by performing similar functions
- Interdependencies: one business activity feeds into another business activity
- Near Monopolies: a small number of companies provide the same essential product or service to an entire industry

In many Critical Infrastructure industry sectors there are very few "Redundancies" and many "Interdependencies" and "Near Monopolies". There is also a significant risk of overloading beyond system specification.

A classic example of a cascade initially affecting the power supply occurred in August 2003, affecting 45 million people in eight US states and a further 10 million people in Canada. A generating plant in Ohio went offline as a result of high demand in hot weather. This put strain on high voltage lines that came into contact with insufficiently trimmed trees. A race condition developed in a computerised energy management system owned by General Electric, triggering an alarm system. The load was transferred to a back-up system which itself failed, triggering a

series of failures over the next four hours. Other power plants went into "safe" mode, and over 500 generating units became unavailable. In addition, the water supply failed in places because pumps needed electricity. Rail services in and out of New York City and much of the US north-east stopped. Cellular communications were disrupted when back-up generators ran out of fuel. Large numbers of factories had to close and border crossings between the United States and Canada became difficult because it was no longer possible to use electronic checking systems. There were also reports of looting in Ottawa and Brooklyn, New York (U.S.-Canada Power System Outage Task Force, 2004).

In the telecommunications sector, emergencies can trigger great demands on landlines, mobile phones and on the Internet, both in terms of access to facilities and to particular websites that normally provide public safety information.

For most forms of cybercrime or cyberattack to succeed there must be a significant sequence of research, deployment and implementation. Unless all the ingredients are present, there will be no success. Thus:

- A "phishing" attack consists of:
    - An inducement to a victim to accept an email or weblink
    - A Trojan which, once implanted, requires some-one to task it to find usernames and passwords, or
    - A fake website which will collect usernames and passwords
    - Some-one to organise the process by which the usernames and passwords are used to collect funds – which must be done so as to avoid detection during the act and leave no trace to the fraudster/beneficiary
- A DDoS / Extortion requires
    - The crafting of a DDoS exploit which is not likely to be detected by regular preventative security tools
    - The assembly of a BotNet to mount the attack – and which will not lead back to the organiser
    - Research on the computer systems of the intended victim, including any back-ups
    - The making of the extortion demand and the setting up of a communications channel which will not identify the blackmailer
    - A means of collecting extorted funds but which will not identify the blackmailer
- A SCADA-based attack requires
    - Knowledge of security weaknesses in specific hardware
    - A tool which will exploit that weakness
    - Knowledge of the physical location and IP addresses of each SCADA device to be attacked
    - Research into the likely extent of effects.

These are of course simplifications of the elements actually required and the examples are of "regular" semi-localised events and not global threats.

The analysis by Symantec of Stuxnet which targets SCADA devices (Falliere, 2010) shows what is involved in designing highly targeted malware. There are at least four different components: how the attack choses industrial control systems to target, the method used to infect a specific programmable logic controller (PLC) data block, the actual code that is placed onto the PLC during infection, and the rootkit that is present on an infected Windows machine. Stuxnet involves several zero-day exploits plus a great deal of intelligence gathering. (O'Murchu, 2010)

Appendix 1 of this study attempts an exploration of a number of potential feasible global cyber hazards, analysing them for Triggers/ Likelihood of Occurrence/ Ease of Implementation, Immediate Impact, Likely Duration / Recovery factors – immediate, Propagation, Likely Duration / Recovery factors – Longer Term, and Potential for Global Impact. The purpose is not to make precise forecasts or to produce an exhaustive list, but to build an understanding of some of the key mechanisms and risk factors. Some of the events described as a "failure" or a "compromise" are neutral as to whether the cause is deliberate or accidental – the focus is on effects.

It will be seen that, once the scenarios are played through, almost none of them actually qualify as a likely global shock, although in some instances the local and short-term effects can be considerable. There are a number of reasons why cyber-events do not necessarily reach a tipping point from which there is a cascade into a more global event, among them:

- The Internet was designed from the start to be robust and self-healing, so that failures in one part are routed around
- The same is true of the main physical telecommunications infrastructure – there can be local failings but all other traffic will find alternative, albeit slightly slower, routes
- In many cyber-events there is no loss of physical resource; what may need to be rectified is vulnerable software or data
- Historically, solutions to discovered flaws in software and operating systems and/or the emergence of new forms of malware - have been found and made available within a few days
- Again, historically, few single DDoS attacks have lasted more than a day; this seems to be because defensive signatures are fairly rapidly derived and because the longer an attack lasts the greater the opportunities for trace-back techniques to identify perpetrators
- Many government departments and major businesses and organisations have ICT-related back-up and contingency plans
- If a single large commercial or NGO entity such as a bank or health-care provider is incapacitated, there is often some rival alternative organisation that take on some of the essential traffic
- Although their usage is not as universal as one may like, large numbers of government departments and major businesses and organisations and private individuals do deploy up-to-date malware detection, firewalls and intrusion detection technologies. The consequence is that would-be perpetrators must constantly find new exploits if they are to be successful.
- Many of the networks transmitting the most important data, for example about world financial transactions, are not connected to the Internet, use specialised protocols and equipment, and have reasonably strong levels of access control. Any compromise requires insider knowledge

Local loss of internet and telecommunications capacity – or even power and water supplies - for a few days, while causing possibly great inconvenience and some financial loss, does not qualify as a "global shock".

However this is simply to look at grievous single cyber-events in isolation.

Appendix 2 considers the position where there is an existing "conventional" disaster and a coincidence of some form of cyber-event. What happens if a country is already weakened by a disease pandemic and there is a failure of Internet facilities or malware which incapacitates personal computers? In the event of a very large-scale fire, flood, chemical escape, or earthquake, what would be the impact if Internet connectivity was not available, for example to tell the authorities where help was needed, to assist victims in obtaining help and to enable the public to check on the welfare of friends and family?

Here the analyses help reveal some of the dependencies and relationships.

A further interesting outcome is that it is a mistake to try and rank likely cyber catastrophes in terms of triggering events. In other words one should not try to estimate whether a DDoS attack is "worse" than one on SCADA systems or exploitation of a zero-day fault or physical loss of a main communications switch. The issue is, in any one event, the likelihood of propagation and cascade – and these will vary considerably even for the same triggering event.

In terms of mounting a successful cyberwar, that is, where nearly all the action takes place in cyberspace and there is almost no kinetic element, one has to conclude that a whole succession of carefully crafted and researched techniques would be required.

We explore some of these factors more fully in the next section.

Y2K and the Millennium Bug

During the 1990s there was widespread global concern that critical information systems might fail in the run-up to the year 2000 due to difficulties in processing dates in the new millennium. The US Commerce Department estimated that preparations for this "Y2K" event cost American government and industry USD 100 billion between 1995-2001, and that other countries likely spent at least this amount again. As with cybersecurity risks, there were concerns that individual actors would rationally underspend on remediation efforts as the cost of system failure would partially be borne by other interdependent organisations (Mussington, 2002: vii—viii).

There was widespread bilateral and multilateral governmental and industry cooperation to share information and galvanise action and contingency planning. The immediacy and obvious nature of the threat persuaded organisations of the necessity of a serious and well-resourced response. A US government review concluded "the processes and institutions responded to a common threat in a manner that successfully mitigated the potentially disastrous consequences of a unique and severe technological problem," while calling for further research into "networks, infrastructure interdependencies, economic criticality, and the likelihood of vulnerability exploitation" (Mussington, 2002: ix).

However, countries that undertook significantly less preparation than the US and UK, such as Italy, Spain, Greece, Russia, Indonesia and nations in Latin America and Eastern Europe, saw no significant systems failures, leading to questions over the ultimate impact of Y2K

programmes (Quigley, 2004: 811) and whether they were sufficiently targeted at the areas of greatest risk. In the UK public sector, Quigley found that "more than half of those interviewed said that their department/agency did not conduct any formal cost-benefit analyses or risk analyses as part of their Y2K plans" (2004: 812). This is particularly significant in complex IT systems where "Errors are not randomly distributed. Only a relatively small amount of effort, well directed, is necessary to avert a very significant proportion of the risk" (Finkelstein, 2000: 157).

There does seem to be a consensus that much of the remediation work undertaken was necessary for the overall stability of information systems. In the UK public sector, Quigley found that "IT departments did not have a reliable inventory of their organizations' systems as a whole, nor did they know how some of the systems worked, let alone if the systems had any date-functionality built into them which might cause systems failures during year-2000 date processing" (2004: 809). Thomas commented that "the lack of … basic quality management (was) responsible for about half the cost of Y2K programmes" and that "enough faults were found and problems averted to justify the time and cost of the work" (2000: 159).

Another relevant lesson for the management of systemic cybersecurity risk was the role of the press, which carried a high frequency of "hysterical media headlines – healthcare crises; aviation disaster; nuclear explosions… Virtually none of the groups involved questioned with sufficient rigour the assumptions upon which Y2K was predicated" (Quigley, 2004: 824—825).

The Problems of Planning a Cyberwar

For a cyberwar to succeed there needs to be a succession of different, persistent attacks on a several targets, the consequence of which is that each individual attack has a magnifying effect. This is the vision of writers such as Richard Clarke. (Clarke and Knake, : 2010, 64). Are these projections feasible?

Single DDoS attacks usually only last 1 -2 days; thereafter the specific attack signature is likely to have been identified and a remedial, blocking technology constructed. In addition, the longer an attack persists, the greater the chance that trace-back activity by investigators will succeed in identifying the perpetrator.

Thus, for an attack to be effective, a great deal of preparatory work is required. If DDoS is the weapon, you need to know the IP addresses of the computer systems or targets; it would also help to know about their operating systems and applications – and what forms of protection and back-up are in place. You will need to have a *successive* series of never-used-before crafted DDoS attacks each with command-and-control system as well as a sub-servient botnet as each individual attack loses its effectiveness. (If you re-use known attack tools you run the risk that your target's anti-malware and intrusion detection systems will spot them before they have any effect) You also need to know what services and functions the attacked system provides so that you can estimate the likely effects – immediate and consequential. Much of this information is also required if you are to attempt to use embedded malware (booby-trapped or infected hardware) as your attack vector.

All this implies a great deal of accurate research and preparation. And you will have to do this for a number of very different systems if you are to manufacture your "perfect storm" conditions. Moreover, most of the time you will be limited to computer systems that are connected to the Internet; to reach proprietary non-Internet connected computer facilities you will almost certainly need significant insider help – which will have had to be recruited.

The larger your ambitions for your attack, the greater the need to research the possibility of unintended consequences – that the cascade of events you hope to trigger does not stop where you want but goes on to overwhelm you and your interests as well.

Finally, as in all wars, you have to think about the end-game: as the thermonuclear analysts had to consider during the Cold War, what will be left? And, on a slightly lesser scale, if you want your enemy to surrender – how will they do so if you have cut off their means of communication and decision-making?

Risk analysis and the broader context

Impact, scope and duration

As we have seen, the most significant cybersecurity risks are related to the non-availability of critical services provided by information systems connected over the global Internet. Advanced economies are increasingly dependent upon these services, and their non-utilisation will have substantial impact on individuals, businesses and governments. Significant risks are related to psychological effects upon individuals and loss of productive output from business and government. Only in very specific circumstances, related to critical national infrastructure, is there any possibility of injury and loss of life or damaged and destroyed property.

Individuals, businesses and governments all face a wide range of cybersecurity risks to their own interests. However, only a subset of these risks has the potential to widen into systemic risks to society. Even these, though, may not be true "global shocks".

Threshold, tipping, trigger and control points

As we have also seen, a common enabler of these systemic cybersecurity risks is the very large numbers of Internet-connected personal computers that have been compromised by malicious software.

A second common threshold condition for systemic cybersecurity risks is the misalignment of incentives of individuals and businesses away from socially optimal conditions, resulting from incomplete information and spill-over costs and benefits of security-related decisions by market actors. Individuals and businesses may rationally under-spend on security protection if the costs of that decision fall mainly on others; but in the increasingly interdependent networked economies of the developed world, "such deviations from optimal security decisions may cascade through the whole system" (van Eeten and Bauer, 2008: 16). For example, software suppliers are principally concerned with the direct costs and benefits of improving the security levels of their products. While there will be some reputational benefit to increased security, it is unlikely to fully offset the private costs of increased security. Network effects in information markets create a first-mover advantage that encourages suppliers to rush to market rather than spend time fully testing the security of new products. Combined with high fixed costs, they often lead to the dominance of a small number of firms and their products, which further increases systemic vulnerability through a "monoculture" effect (van Eeten and Bauer, 2008: 21). The widespread use of insecure software is the main factor behind the compromise of the millions of personal computers that make up the "botnets" used in crime and cyber attacks.

The impact of these security decisions is particularly striking given the extent to which they remain within the control of individuals and organisations:

> *"Errors can be corrected, especially if cyberattacks expose vulnerabilities that need attention. The degree to which and the terms by which computer networks can be accessed from the outside (where almost all adversaries are) can also be specified. There is, in the end, no forced entry in cyberspace. Whoever gets in enters through pathways produced by the system itself." (Libicki, 2009: xiv)*

Social Unrest Factors

How might a substantial and sustained breach of cybersecurity might lead to social unrest? For convenience we set out what we take to be the main generic triggers for social unrest. Prolonged non-availability of Internet services may play a role in some of these, particularly in relation to lack of access to cash and in government-to-citizen communications:

- Uncertainty about the availability of food and water
- Uncertainty about the availability of shelter
- Uncertainty about the availability of electric power
- Lack of access to cash / fear that savings etc may have been lost
- Inability to know about government etc attempts at recovery / remediation
- Inability to contact family and friends
- Fear of spread of disease / lack of medical support
- Fear of breakdown of law and order
- Fear that government does not adequately care for the welfare of a group or community to which victims belong

However, social unrest in any specific situation depends on many other factors, for example the resolve and skill with which a government appears to be handling a crisis – and pre-existing levels of public trust in their government, police and armed forces.

Duration Issues

Pure cybersecurity risks tend to be localised and temporary rather than global and long-term. This is for two fundamental reasons:

1. The longer an attack persists, the greater the likelihood it will be detected, routed around, and become attributable to a specific party against whom actions can be taken (including disconnection, arrest and retribution).
2. Larger-scale attacks result in more of the data needed to diagnose and fix system vulnerabilities, and provide a stronger incentive to system suppliers and administrators to do so (Libicki, 2009: xiv).

Even for the best-resourced and most determined attackers – nation states taking military action – these conditions are likely to hold. RAND Corporation recently reported to the US Air Force "operational cyberwar has an important niche role, but only that", commenting:

> *"Investigation may reveal that a particular system has a particular vulnerability. Predicting what an attack can do requires knowing how the system and its operators will respond to signs of dysfunction and knowing the behaviour of processes and systems associated with the system being attacked. Even then, cyberwar operations neither directly harm individuals nor destroy equipment (albeit with some exceptions). At best, these operations can confuse and frustrate operators of military systems, and then only temporarily. Thus, cyberwar can only be a support function for other elements of warfare, for instance, in disarming the enemy" (Libicki, 2009: xiv—xv).*

Even so, successful attacks on critical information infrastructure can have a significant impact on the day-to-day activities of individuals, businesses and government across large regions largely because of the likelihood of cascade effects. For individuals and businesses,

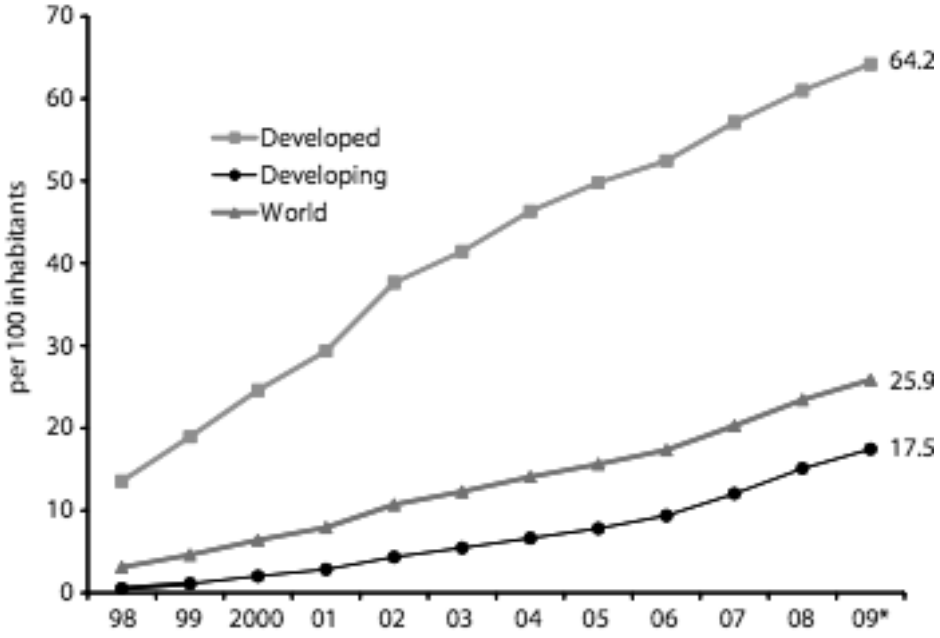
communications and access to information and online services such as banking are increasingly dependent on the Internet. For governments in advanced economies, the United Kingdom's Cyber Security Operations Centre predicts: "Reliance on the Internet as the main means of delivering public services will quickly reach the point of no return, as taking advantage of the cost savings will involve cutting the staff who would be needed to revert to providing services by traditional methods" (2010: 7).

Individuals

The Internet has quickly grown into an essential platform for individuals to interact with friends, family, businesses and governments. Usage has grown by six per cent per annum since 2007 in the developed world, to 64.2% of the population. Younger and better-educated adults are overwhelmingly Internet users: within the EU, for example, this includes 89% of university-educated individuals and 91% of those aged 15-24 (ITU, 2010).

In the same time period Internet usage grew annually by over 21% in the developing world, to 17.5% of the population (ITU, 2010). Globally, developing countries now account for over half of the Internet's users (UNCTAD, 2009).

Figure 6 – Internet Users per 100 Inhabitants 1998-2008



Source: ITU (2010: 2)

Individuals in advanced economies increasingly rely on the Internet to go about their daily lives. A recent large-scale UK survey (Dutton, Helsper and Gerber, 2009) found that 30% of Internet users considered the Internet as their principal source of information, compared to 11% for television, 7% for newspapers and 6% for radio. It would be possible for misinformation to be spread via compromised news sites, although the number and variety of online news sources mitigate this risk.

The same survey found that 65% of users turned first to the Internet for information related to a professional, school or personal project. 55% of users banked online, while 59% had made use of at least one e-government service in the previous year. The United Kingdom's Cyber Security Operations Centre predicts that by 2015, high-speed Internet access will be "essential to people's ability to carry out their daily lives" and that service interruptions will have a "serious impact" on the economy and public wellbeing (2010: 7). Non-availability would reduce people's ability to purchase goods and services; to carry out financial transactions; to plan and book travel; and to communicate with family and friends. In an emergency, it would also impair

their ability to receive up-to-date information and hence co-ordinate their response appropriately.

Businesses

Internet-specific businesses have become a significant contributor to advanced economies. Using an employment-income approach, Hamilton Consultants estimated that the advertising-supported Internet contributes about USD 300 billion, roughly 2%, of U.S. GDP. As an independent economic unit, they estimated that the Internet "exports" an economic value of USD 175 billion per annum to the US economy (2009: 4). The European Commission estimated the European e-commerce market in 2006 to be worth EUR 106 billion, with 70% of revenues concentrated in the UK, Germany and France (2009). Clearly, any disruption in consumer access to online services has the potential to cause significant immediate losses to these businesses. E-commerce levels have continued to grow despite a corresponding increase in fraud levels, which so far have been borne largely by businesses and payment intermediaries.

Beyond the e-commerce market, networked systems are involved in some part of the value chain of virtually every transaction, whether in networked cash registers, payment systems or logistics firms' delivery route optimisation. Procurement packages for both commercial off-the-shelf and bespoke goods have been equipped with Internet access features. Industry supply chains are critically dependent on the information systems used to monitor stock levels, place orders, and coordinate the movement of products from factory floors to retail outlet shelves. These information systems can dampen sudden fluctuations in one part of a supply chain, reducing their systemic impact. Chains are often dependent at specific points on small numbers of firms that provide vital components or services (Borg, 2005).

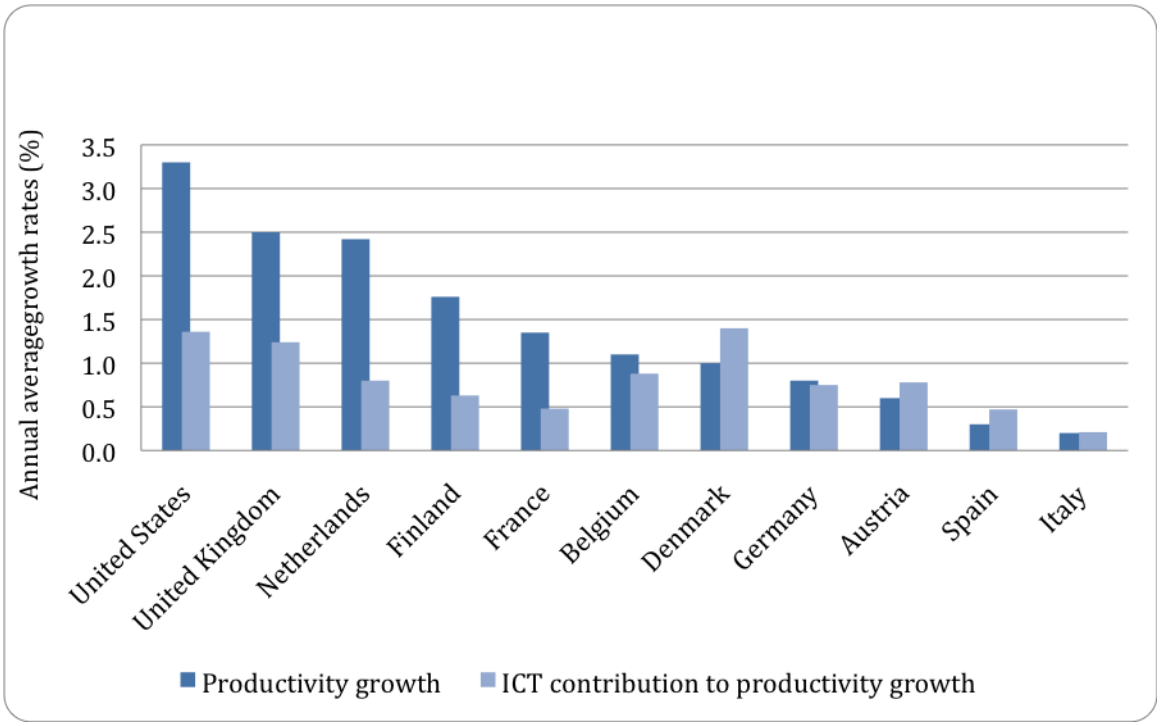
As we have seen, just-in-time, "lean" delivery systems prevalent in the supermarket industry have reduced costs by minimising buffer levels of stock and redundancy in transport systems. They are therefore easily disrupted by problems in transport and communications networks. Public panic buying can quickly magnify these disruptions. During the 2000 fuel protests in the UK, some food stores introduced rationing (Wintour and Wilson, 2000).

Businesses increasingly rely on Internet-based services for internal and external communications. 93% of EU enterprises with at least ten employees have Internet access (Eurostat, 2010: 3). Telecommunications companies are moving their separate voice, video and data networks towards converged Internet-based architectures. Disruption of the communications infrastructure therefore can have a wide-ranging negative impact on business activity. Depending on the architecture of communications networks, damage at one point can have a significant effect elsewhere – as in the recent flooding of a London exchange, which knocked out telecommunications and payment processing for thousands of local customers but also affected 437 other exchanges around the UK (BBC News, 2010).

More broadly, ICT has had a significant impact on productivity growth across the OECD. In some Member countries such as Austria, Denmark and Spain, it contributed over 100% of productivity growth between 1995 and 2004 (OECD, 2008a: 27). According to the European Commission, ICT was responsible for 50% of overall productivity growth in the EU economy for the ten years up to 2004, while the ICT industry itself drove 20% of the total productivity increase across the economy (Reding, 2008).

If business fears over cybersecurity reduce investment in ICT, this could have a significant long-term impact on productivity growth. Similarly, consumer cybersecurity fears may impede the transition of many financial and other transactions to much cheaper online platforms. This would represent a significant loss of cost savings to individual businesses and to society of economic efficiency gains and accelerated growth (van Eeten and Bauer, 2008: 7—8).

Figure 7 – Contribution of ICT capital growth to labour productivity growth in market services (1995-2004)



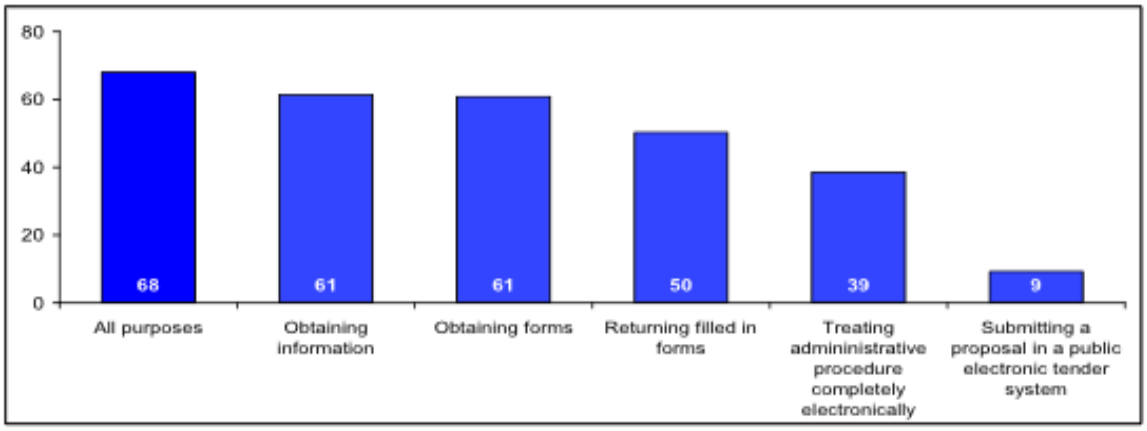
Source: OECD (2008a: 27)

Government services

Most OECD governments are moving to take advantage of the efficiency and performance improvements available through using online channels to deliver services to citizens and businesses, and to modernise their own internal processes. In 2007 32% of citizens in OECD Member countries interacted with public authorities using the Internet. Top-performing states such as Norway, Iceland and Denmark dealt with almost 60% of citizens electronically (OECD, 2008a: 18).

Current fiscal constraints are leading to a renewed emphasis from governments on this transition. The UK estimates that reducing local government inefficiencies using the Internet could achieve annual savings of over GBP 600 million (Denham, 2009), with another GBP 600 million in savings through eliminating face-to-face contact in provision of some services by 2014 (HM Treasury, 2009a).

Figure 8– Enterprises using the Internet to interact with public authorities, by purpose, during 2007, EU27 (%)



Source: Eurostat (2008: 2)

While many interactions with government are not time-critical, any sustained disruption of online services could delay vulnerable citizens in claiming social security benefits and hinder businesses in filing tax and other administrative returns. Two-thirds of EU businesses already interact online with government.

Governments play a key role in coordinating responses to large-scale emergencies, and are as dependent as businesses on communications infrastructures to do so. The European Network and Information Security Agency is planning a cross-EU exercise during 2010 to ensure EU member states are able to cope with a simulated loss of connectivity while still providing key services (European Commission, 2009).

A further problem is that much government computing may be outsourced, the computers themselves run by commercial third parties against a tightly-written Service Level Agreement, which may not anticipate what might happen in catastrophic circumstances. In the United Kingdom the extent of reliance on outsourcing and its role in official policy can be seen from the Treasury's *Operational Efficiency Programme:* (HM Treasury, 2009b). The language used is of efficiency and savings for the taxpayer and the concern must be that some "savings" are achieved by not spending adequately on security and resilience. Government out-sourcing contracts have been regarded as "commercially sensitive" which means that neither the detailed specifications nor the obligations of the supplier are available for scrutiny. There does not appear to be any formal requirement during the procurement process for the UK government's security and resilience specialists to provide analysis and criticism.

Critical National Infrastructure

As we have seen, while there have so far been few electronic attacks on Critical National Infrastructure, there as been significant concern that insecure Internet-accessible SCADA systems could be used to overload power grids, block communications and financial transfers and even lead to "all of North London's sewage suddenly shooting on to the Olympic site" (House of Lords EU Committee, 2010: 100) (Clarke and Knape, 2010: 97-101).

Without an example of a large-scale cyber-attack on critical infrastructure, one way to estimate damage is to look at costs associated with past failures due to overload or an external shock that interrupted service. California's electricity crises of 2000 and 2001 provide one of the few large-scale examples of the failure of large-scale critical infrastructure. Despite global media coverage of blackouts, outage rates did not vary significantly from those of the power companies during the 1990s. Blackouts occurred on eight days for 27 hours. On key variables the system operated closer to failure than usual, but the Independent System Operator mostly maintained acceptable levels of reliability. De Bruijne and van Eeten estimated the total social costs of the outage at USD 60-USD 70bn (2007: 27).

Fraud

As transactions and payments are increasingly made online, fraudsters have unsurprisingly adapted techniques to dip into these new financial flows.

There is little doubt that the highly organised types of fraud similar to "phishing" will continue to develop. Direct attempts at defrauding or compromising bank computer systems also have a long history. Vladimir Levin and a group of St Petersburg hackers attempted to remove USD 10.7 million from Citibank in 1994 (Bugtraq, 2001). In 2004 keyloggers were used against Sumitomo Mitsui Banking Corporation in London in an attempt to move GBP 229 million to 20 accounts in 10 different countries. (Young, 2009) There are also

many examples of runs on banks, though historically most of these have been precipitated by bad lending or failure to anticipate changed economic conditions.

The issue is how far these activities might impact on a "global shock" scale. A potential risk remains that more successful criminal activity will "tip" these conditions into a systemic consumer distrust of online banking and payment systems and unacceptable costs of fraud for businesses, as well as providing an increased funding stream for other criminal activities.

Espionage against states, businesses and NGOs

Much less obvious than online fraud are intelligence-gathering operations conducted against states, high-technology businesses and non-governmental organisations. Intelligence agencies, large companies and "patriotic hackers" have a strong incentive to break through access controls on Internet-accessible systems that contain sensitive government, commercial and campaigning information. The Center for Strategic and International Studies has warned: "Porous information systems have allowed our cyberspace opponents to remotely access and download critical military technologies and valuable intellectual property… that cost billions of dollars to create" (2008: 13).

One series of incursions received unusual media prominence in 2005, with reports of an FBI investigation (codenamed "Titan Rain") into hackers apparently located in the Guangdong province of southern China. A security analyst at Sandia National Laboratories monitored data being stolen on subjects such as NASA's Mars Reconnaissance Orbiter and Air Force flight-planning software. As well as non-classified US government systems, the hackers accessed systems at the World Bank and at defence contractors such as Lockheed Martin. Defence, law enforcement and intelligence agencies in the UK, Canada, Australia and New Zealand alerted business to improve security procedures in light of these intrusions (Thornburgh, 2005). It was not clear whether there was any state involvement in these attacks, although more generally the US-China Economic and Security Review Commission concluded:

> *"The depth of resources necessary to sustain the scope of computer network exploitation targeting the US and many countries around the world coupled with the extremely focused targeting of defense engineering data, US military operational information, and China-related policy information is beyond the capabilities or profile of virtually all organized cybercriminal enterprises and is difficult at best without some type of state-sponsorship" (2009: 8).*

More recently there have been specific allegations of espionage against dozens of Chinese human rights activists' Google mail accounts, causing Google to withdraw from the Chinese mainland; and against the Dalai Lama's office, where 30 of 50 computers were infected with software that was sending confidential information back to China (Information Warfare Monitor, 2009):

> *"It was clear that this was an action, in effect, of the Chinese State, because the intelligence product was used by Chinese diplomats on more than one occasion when the Dalai Lama's staff were arranging for him to meet foreign dignitaries. The dignitaries were contacted by Chinese diplomats and warned off. Had it not been for that, then perhaps there might have been some difficulty in attribution." (House of Lords EU Committee, 2010: 11)*

Military espionage is a systemic risk only in the sense that it may alter the balance of tactical and strategic capabilities between opponents and hence the ability of states to project hard power. Economic and political espionage are systemic risks in the long term: they reduce the resource advantage, technological leadership and ultimately power of high-tech economies; and hamper the ability of non-governmental organisations to successfully campaign for democratic values.

Signals intelligence and military agencies and defence contractors generally have highly developed capabilities to defend military and intelligence networks. It is the proliferation of sensitive information in non-classified systems elsewhere in government, business and non-governmental organisations that presents a challenge in limiting digital intrusions. Measures widespread in the former, such as secure software development procedures, strong enforcement of access control mechanisms and the routine use of encryption, can all reduce the ability of attackers to gain unauthorised access to systems and data. However, they are resource intensive and often user-unfriendly if not carefully designed.

Attacks on critical infrastructure availability

The threshold condition for cybersecurity risks in the availability of critical infrastructure is insecure access controls on systems controlling power and water grids and the information services relied upon by payment systems, emergency responders and major food suppliers. This includes physical access restrictions to reduce the risk of damage to computer hardware and cabling, and good practice in the management of system security. Most importantly, such services should be (and generally are) inaccessible from the public Internet.

The attacks on government, banking and media websites that have been seen in Estonia, Georgia, Lithuania and South Korea illustrate the potential problems if more critical services are made publicly accessible. However, it is highly questionable whether any of these attacks justify the label of "cyberwar":

> *"The 'Korean' cyber incidents of early July did not rise to the level of an act of war. They were annoying and for some agencies, embarrassing, but there was no violence or destruction. In this, they were like most incidents in cyber conflict as it is currently waged. Cybercrime does not rise to the level of an act of war, even when there is state complicity, nor does espionage – and crime and espionage are the activities that currently dominate cyber conflict... Cyber incidents in Estonia and Georgia also did not rise to the level of an act of war. These countries came under limited cyber attack as part of larger conflicts with Russia, but in neither case were there casualties, loss of territory, destruction, or serious disruption of critical services. The 'denial of service' attacks used against these countries sought to create political pressure and coerce the target governments, but how to respond to such coercion remains an open question, particularly in light of the uncertain attribution and deniability" (Lewis, 2009: 2—3).*

So long as critical infrastructure is isolated and well-protected, cybersecurity risks are reduced to a level that likely can only be triggered by attacks from sophisticated nation state adversaries such as the US, China, Russia, France, Israel and the UK. Writers such as Lewis (2009: 7) have observed that a successful attack on infrastructure "requires planning, reconnaissance, resources and skills that are currently available only to these advanced cyber attackers." Libicki noted that other potential attackers have not been held back by lack of motivation: "adversaries actively engaged against the United States (who thus have no reason to hold back for a more propitious time) have not conducted known cyber attacks; examples include Serbia in 1999, Iraq in 2003, and al Qaeda since at least 1998" (2009: 37).

Such attacks also have the potential to provoke heavy reprisals. Lewis (2009: 7) observed: "there are remarkably few instances of a nation engaging in covert sabotage attacks against another nation (particularly larger powers) unless they were seeking to provoke or if conflict was imminent. The political threshold for serious cyber attack (as opposed to espionage) by a nation-state is very high, likely as high as the threshold for conventional military action."

However, a strategy of deterrence is of limited value when the origin of attacks can be extremely difficult to attribute with any confidence. The denial of service attacks on Georgia, which occurred during military clashes with Russia, are a case in point: "the peak size of the attacks was substantially larger than the attacks on Estonia the year before, (but) we simply do not have the evidence to attribute any of these attacks to a specific group or a

Government agency. On the contrary, analysis of the data suggests non-State actors." (House of Lords EU Committee, 2010: 11)

More effective is increasing the resilience and robustness of critical systems, and societies in general. It is for this reason that we devoted earlier passages in this study to an examination of how state contingency plans need to operate and develop. Adding redundancy to systems allows some service to be continued while damaged components are isolated, repaired and replaced (Libicki, 2009: 162). There are many historical examples of societies that have proven robust even to extreme pressure on essential services:

> *"Few nations have yielded to trade embargoes alone, even to universal trade embargoes. It is unclear that a cyberwar campaign would have any more effect than even a universal trade embargo, which can affect all areas of the economy and whose effects can be quite persistent. Even a complete shutdown of all computer networks would not prevent the emergence of an economy as modern as the U.S. economy was circa 1960—and such a reversion could only be temporary, since cyberattacks rarely break things. Replace "computer networks" in the prior sentence with "publicly accessible networks" (on the thinking that computer networks under attack can isolate themselves from the outside world) and "circa 1960" becomes "circa 1995." Life in 1995 provided a fair measure of comfort to citizens of developed nations." (Libicki, 2009: 123)*

Where critical systems cannot be isolated from the public Internet, a high degree of redundancy will greatly reduce the risk of a service being completely knocked out. For example, government websites providing public advice and reassurance during a crisis could be replicated across the tens of thousands of servers operated by Content Distribution Networks such as Akamai. The Internet's Domain Name System, which translates human-readable addresses such as `oecd.org` into numeric Internet Protocol addresses, is distributed across an extremely large number of servers across the Internet. The system runs 13 "root server" clusters, some of which are distributed across different continents using the "anycast" load balancing protocol. These proved highly resistant to a distributed denial of service attack in 2007, with a review by the Internet Corporation for Assigned Names and Numbers concluding: "Even though it was a large attack, the new (anycast) technology, combined with the speed, skills and experience learnt by root server operators over the years, helped to make sure that actual Internet users were not inconvenienced" (ICANN, 2007).

Since mid-2010 attack on the DNS root servers has been made more difficult as a result of the deployment of DNSSEC, which requires that all interactions are authenticated via digital signatures. (www.dnssec.net). However while this method makes the spreading of false DNS data much more difficult, it still does not directly address the problem of maintaining availability. Work still needs to be carried out to secure the Border Gateway Protocol (BGP), which is the protocol that establishes routing information on the Internet. There are proposals for a Secure BGP (S-BGP) which uses a public key infrastructure to thwart IP address spoofing. (Kent, 2006) (ENISA, 2010)

Malware and "Global Threats"

There is little doubt that the sophistication of malware (and its close relative cyberweaponry) is increasing all the time while the levels of skills to deploy continue to drop. There is also no doubt that the Internet acts as a high-speed vector for the distribution of information on system vulnerabilities and their exploitation. Nor is there any doubt that a substantial marketplace of exploitative tools operates. The question though, is how far these phenomena amount to a potential tipping point.

Little malware, even if it hits large numbers of victims, can be considered a "global threat" in the sense of causing disruption at the level of the nation state. Moreover not all unpleasant payloads can be regarded as weapons, in the sense of directed, controlled, force.

The conventional virus/Trojan such as Conficker.C, Slob.Trojan, Storm worm, or from earlier times, SQL Slammer, MyDoom, Sasser and Netsky, may cause considerable upset to individual computer users, but often does not measurably disrupt national productivity. Because of the means of transmission – via the Internet but without discrimination as to target and succeeding only where anti-virus precautions have not been taken or have proved inadequate – targeting is extremely inaccurate and there is a considerable risk that "friends" of the perpetrator are affected as well. Stuxnet was not a single item of malware but a carefully crafted combination of several different forms and it also relied on very specific knowledge of its apparent selected targets. (O'Murchu, 2010).

Malware and the Internet economy

In a background report for the 2008 Ministerial meeting in Seoul, the OECD warned that a global partnership was needed to prevent malware becoming a serious threat to the Internet economy. This would include actions to improve understanding, organisation and allocation of responsibility by a broad community of public and private sector actors. Alongside governments, action was needed from Internet Service Providers, e-commerce companies, domain name registrars, software vendors and end users. These market players have mixed incentives to improve security, with costs frequently falling on other actors in the value chain.

Current responses to malware are mainly reactive. The OECD suggested greater national and international "structured and strategic co-ordination" to assess and mitigate risk. This cooperation would improve the quality of data on the "scope, trends, development and consequences" of malware, and hence the accuracy of assessments of its social and economic impact. The report suggests the development of "joined-up policy guidance" by governments, the private sector, the technical community and civil society. This would include action on public education; enhanced technical measures; mutual assistance between law enforcement agencies; and stronger economic incentives for increased security (OECD, 2007: 46—53).

Level of preparedness

Governments, even in advanced economies, have significantly different levels of preparedness for cybersecurity risks and attitudes towards dealing with them. For some the response has been to build up military offensive and defensive capabilities on the basis that the main threat is cyber-attack, which they believe can be deterred. Other countries concentrate on mitigation and recovery – the civil contingencies agenda. Such an approach requires the co-operation of the private sector, especially those businesses delivering essential services with whom a particular set of understandings must be evolved. Many states are looking for international agreements on law and declarations of non-use of cyberweaponry. Governments are also developing a role in educating and preparing their citizens.

One area that seems neglected is the role of technology in mitigating and recovery from destructive hazards of all kinds – and the implications for the design for the resilience of critical government and private sector computing and communication facilities. Computer data is easily backed up so that loss at one site can, provided the appropriate planning is place, be quickly restored at another. A physically destroyed computer is much more easily replaced than the equivalent functions performed by human clerks, again provided that plans have been made. Computers can be used to handle and mediate complex recovery plans for whole organisations including the re-siting of work-places and personnel and can also oversee the switching of telecommunications links and facilities from a compromised location to a safe one. Finally, the Internet provides both the means for recovery specialists to understand the detail of the catastrophe they must address and a route for providing the outside world – stake-holders and the public – with information to build confidence.

Military Responses

The armed forces of nations such as the US and China have made very significant investments in offensive and defensive cyber-capabilities. The United States Department of Defense established a unified Cyber Command responsible for addressing "a growing array of cyber threats and vulnerabilities" and to "secure freedom of action in cyberspace" (US Secretary of Defense, 2009). The first US Cybercom Commander was appointed in May 2010. (http://www.defense.gov/releases/release.aspx?releaseid=13551)

> *U.S. Cyber Command possesses the required technical capability and focuses on the integration of military cyberspace operations. The command is charged with pulling together existing cyberspace resources, creating synergy that does not currently exist and synchronizing war-fighting effects to defend the DoD information security environment. This is not an expansion of DoD's mission. It is in keeping with the department's mission to protect and defend U.S. national security and protect the lives of men and women in uniform.*

Further indications of US pre-occupation with cyber attacks as opposed to accidental cyber events comes in a 2010 report by the US National Research Council: *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* This addresses military and intelligence community perspectives, but not those from business and civilians in general. (NRC, 2010).

A report for the US-China Economic and Security Review Commission recently concluded that the People's Liberation Army strategy included "simultaneous application of electronic warfare and computer network operations against an adversary's command, control,

communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) networks and other essential information systems… PLA campaign doctrine identifies the early establishment of information dominance over an enemy as one of the highest operational priorities in a conflict" (Northrop Grumman, 2009: 7).

In May 2008 NATO established a Co-operative Cyber Defence Centre of Excellence in Talinn, Estonia (http://www.ccdcoe.org/). In July 2010 extensive news reports said that the Indian Army was developing considerable cyberwar capabilities, principally as a response to perceived threats from China. (Times of India, 2010)

High-technology armies, navies and air forces are clearly critically dependent on the security of their information, navigation and communications systems The ability to compromise an enemy's equipment and critical infrastructure as part of wider military action gives a powerful advantage to an attacker. (United States Air Force, 2010). However, the almost-constant uncertainty involved in attributing cyber-attacks and predicting the full impact of counter-strikes requires an adjustment in traditional doctrines of deterrence:

> *"Deterrence relies on more than the implied threat of the use of force in response to an attack. It requires statements about intentions and understanding among potential opponents that define and limit the environment for conflict. Deterrence in cyberspace is limited because we have not adequately assessed what combination of cyber capabilities, defensive measures, and international agreements will make the United States and its allies most secure. It would be useful to undertake a larger strategic calculation, preferably in a public dialogue, to determine the weighting and balance among offensive, defense and multilateral efforts in cyberspace that best reduces the risk of cyber attack." Lewis (2009: 5)*

There are further problems with a military-heavy approach. Many of the likely targets will be civilian, often in private ownership. The tasks of hardening these against attack and responding when an attack takes place will fall most immediately on the owners; there is almost nothing in conventional military training which would qualify soldiers for the role. It is even less clear how the military could build a capability to withstand attacks on civilian targets. Few countries seem to have thought through the intended relationship between the military and civilian realms.

An advisor who served in the White House for Presidents Reagan, Clinton and both Bushes, castigated current United States doctrine thus:

> *At the beginning of the era of strategic nuclear war capability the United States deployed thousands of air defence fighter aircraft and ground based missiles to defend the population and the industrial base, not just to protect military facilities. At the beginning of the age of cyber world war the United States government is telling the population and industry to defend themselves.* (Clarke, R A and Knake, R K: 2010: 144).

Clarke blames a widely-held perspective in the United States against "big government", a concept which can include opposition to regulations mandating security standards and situations in which the federal government may need to issue instructions to private companies.

Clarke's book describes at length the succession of cyber security initiatives in the United States and the turf-war between various entities: the White House, Pentagon, National Security Agency, Department of Homeland Security as well as the Navy, Army, Air Force and Secret Service.

But even he concentrates on situations which might be described as "war" or "attack" whereas, as we have seen, significant cyber-events can be triggered by accident or software

failures. The role of the military in addressing these seems even less obvious. In the United States and in the United Kingdom efforts are being made to make military and civilian personnel work together in the same institutions and it will be interesting to see how these arrangements work out. In July 2010, the US General Accountability Office in its *Global Cybsersecurity Challenges* lamented the number of US agencies that had some role in cybersecurity but which were poorly co-ordinated and where there was lack of clarity over linkages with the private sector. It recommended the need for "protocols for working on cyber incident response globally in a manner that is consistent with our national security interests." (GAO, 2010: 40)

Civil Contingencies

Other countries, among them the UK and the Netherlands, have well-established programmes to deal with a range of large-scale events which might impact the population as a whole. These are being extended to cover cybersecurity events.

In planning for such catastrophes, governments' main concerns are to reduce deaths and injuries, protect property and maintain public order. Costs are a significant concern, since planning and emergency response have to be funded from taxation. A commercial organisation developing a contingency plan normally has almost complete control of the entity it wishes to protect, but governments typically control only part of the landscape that makes up normal life for its citizens.

In 2006 the OECD carried out a comparative analysis of policy approaches as they then existed in four countries, Canada, Korea, the UK and the USA. (OECD, 2006)

Substantial parts of what is referred to as a state's Critical National Infrastructure (CNI) are in private ownership. Earlier we saw a chart of the Dutch vision of the interdependencies. The UK defines CNI as follows:

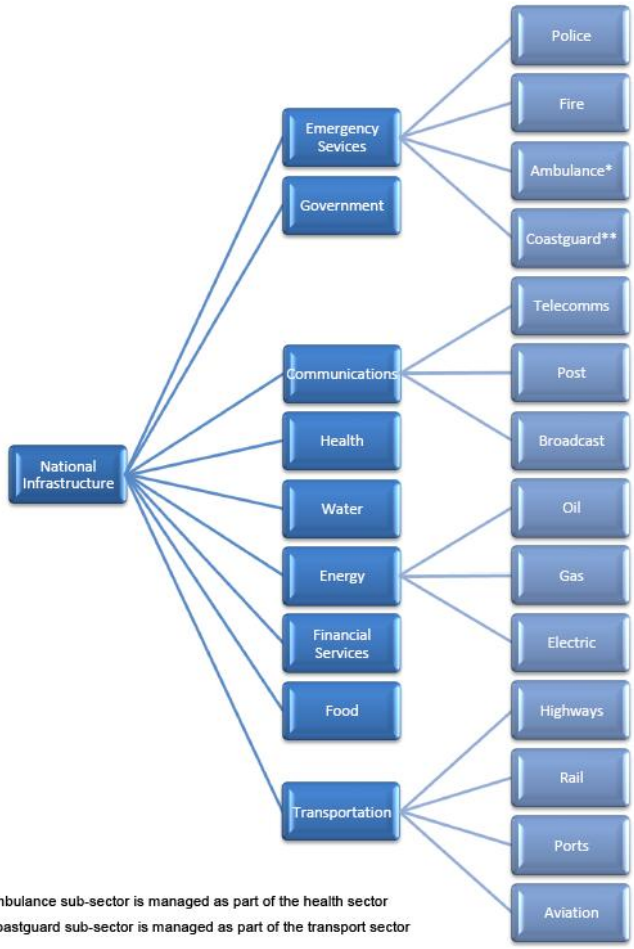
> *those facilities, systems, sites and networks necessary for the delivery of the essential services upon which daily life in the UK depends and which ensure the country continues to function socially and economically. (Centre for the Protection of National Infrastructure, 2010)*

Most other countries use similar definitions. EU Council Directive 2008/114/EC refers to:

> *An asset, system or part thereof which is essential for the maintenance of **vital** societal functions, health, safety, security, economic or social well-being of people, **and the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions***

The UK defines nine national infrastructure sectors which provide these essential services: Communications, Emergency Services, Energy, Finance, Food, Government, Health, Transport, Water (UK Cabinet Office, 2009). Figure 9 shows the categories within these sectors in diagrammatic form:

Figure 9 – UK Critical National Infrastructure



Source: UK Cabinet Office (2009)

However entities such as the UK's Civil Contingencies Secretariat are only part of the picture and it is not clear how they interact with other elements within Government. The linked Office of Cyber Security and Information Assurance (OCSIA) and Cyber Security Operation Centre (CSOC) were set up in late 2009 in the UK to achieve greater levels of co-ordination and strategic analysis. Both units draw their personnel from a number of existing agencies all of which had some interest in cyber security. These include: the Centre for the Protection of the National Infrastructure, Joint Terrorism Analysis Centre, GCHQ/CESG, Department of Business Innovation and Skills, Ministry of Defence, National Fraud Strategic Authority, Foreign Office, Home Office, Serious Organised Crime Agency, and Police Central E-Crime Unit. (UK Cabinet Office. (2009). They have also asked industry and academia to take part in horizon-scanning exercises, to make predictions about future trends in technology, the social and commercial impact, and what the risk landscape might look like in a few years. Both in the United Kingdom and in the United States there have been initiatives to find and develop new cybersecurity skills and identify areas for further research. The UK initiatives are the Cybsecurity Challenge (https://cybersecuritychallenge.org.uk/) and the Cybersecurity Knowledge Transfer Network (https://ktn.innovateuk.org/web/cyber-security). At the time of writing there has been a recent change of government in the UK and a new National Security Council with cybersecurity in its remit has started to work -- £650m of new funding has been allocated.

The 2006 OECD study mentioned the extent to which policy approaches were influenced by local culture. For example, the policymaking environment in the US contends with distrust of government interference in private business. In Korea there are a small number of very powerful private sector companies, while in France the State still retains a share-holding

interest in a number of large CI companies and has not so far followed the UK route of full privatisation.

Private sector

Businesses have clear incentives to manage their own cybersecurity risks, consistent with the level of perceived threat, potential losses, and the cost of system protection. Different business models will result in differing trade-offs for market actors such as ISPs, software companies and financial service providers. In some cases, however, a firm may implement a rational level of protection for their own assets without considering the resulting costs of insecurity that could fall on other parties – such as when infected machines are used to launch attacks against third-party machines.

Van Eeten and Bauer interviewed senior executives across a range of these companies to explore their attitudes to cybersecurity risks. They found significant efforts underway within the information industries to protect customers from these risks, sometimes even where they arose as a consequence of socially non-optimal decisions. ISPs had strong incentives to provide security assistance to customers to reduce the costs of support calls and dealing with abuse notifications, and to protect their reputation with other ISPs and hence reduce their risk of being blacklisted (2008: 26—34). Many software companies have invested heavily in more secure development processes, although their incentives are often stronger to be first-to-market with less secure products. Market leaders such as Microsoft have stronger incentives to invest to protect this position, even sometimes at the cost of backward compatibility problems resulting from security improvements, stemming from reputation protection and the cost of developing and deploying patches (2008: 38—46). Financial service providers can cut costs by two orders of magnitude through moving transactions online. This has proven enough of an incentive for providers to voluntarily cover customers' losses from fraud even in countries that do not mandate such protection (2008: 34—37). Inter-bank payment systems, card and cheque payments and Automated Teller Machines also make heavy use of closed networks that are less susceptible to attack against the wider Internet (House of Lords EU Committee, 2010:154).

Plans to reduce the impact of a successful attack should be part of business continuity planning for all firms. For example: an explosion at a UK oil refinery destroyed the nearby premises of Northgate Information Systems, which runs payroll systems for the employers of 1 in 3 Britons and admissions systems for hospitals across southern England. Despite short-term disruption, good continuity planning minimised the systemic impact of this service interruption (House of Lords EU Committee, 2010: 13). Regulators of the power, water and financial services industries typically require detailed continuity plans to be made and tested regularly.

Concerns remain that the private sector is less well prepared against commercial and state espionage, to an extent that could damage the long-term national competitiveness of advanced economies. The Center for Strategic and International Studies commented in a recent report: "Fleets, armies, and military alliances will not be as important … as the ability for the nation to accelerate its technological progress and economic growth, to create new ideas and products, and to protect its informational advantages" (2008: 12).

Government, Private Sector and Public Private Partnerships

The ownership of the Critical National Infrastructure of OECD Member countries is partly public and partly private. For a wide variety of catastrophes the two elements will need to work together to achieve adequate levels of protection and ability to recover.

The usual way in which this issue is addressed is by reference to "public private partnerships". However there is a significant danger that this phrase remains a description of an aspiration rather than a well-worked out set of formal relationships and understandings.

Government-industry agreements on cybersecurity

There was global media coverage of Chinese attacks on Google's systems in late 2009. In response, the company began negotiating an agreement to share information with the US National Security Agency (NSA) so the two parties could jointly improve the security of Google's networks. The US Director of National Intelligence said that the attacks were a "wake-up call" and that cyberspace could only be protected through a "collaborative effort that incorporates both the U.S. private sector and our international partners" (Nakashima, 2010).

However, intense controversy has resulted in the US over the civil liberties implications of such an agreement. Groups such as the Electronic Privacy Information Center (EPIC) and the American Civil Liberties Union (ACLU) have complained about the "problematic" nature of the agreement. EPIC director Marc Rotenberg commented: "We would like to see Google develop stronger security standards and safeguards for protecting themselves. But everyone knows the NSA has two missions: One is to ensure security, and the other is to enable surveillance" (Vijayan, 2010). The ACLU commented: "Cybersecurity for the American people should not be handed over to a military spy agency, one that is insulated from public oversight and has a history of secretly exploiting vulnerabilities, rather than fixing them" (ACLU, 2010).

Similar controversy has attended a UK intelligence agency "Intercept Modernisation Programme" that includes a contract entitled "Mastering the Internet". This contract would reportedly give intelligence staff "complete visibility of UK Internet traffic" using interception equipment installed across Internet Service Providers' networks. Human rights groups have attacked the programme as a "big brother database" and "network of black boxes", and forced a government retreat on a plan to build a central database of communications records drawn from ISP systems (Leppard and Williams, 2009), (Sommer, and Hosein,: 2009)

While governments and the private sector will need to work together to secure critical infrastructure, effective privacy safeguards and civil society involvement will be required to ensure public trust in these arrangements. A former British Security and Intelligence Co-ordinator put it like this:

> *In the area of security the public has to take a lot from government on trust, and trust is a quality in their relationship that is often lacking in both directions… Since there is no absolute security to be had at an acceptable financial or moral cost in this world, at every stage a balance must be maintained within the framework of human rights based on the time-honoured principles of proportionality and necessity.* (Omand, 2010)

At the heart of the problem is that private sector companies have primary obligations to shareholders and customers, and not a wider "public good". Contingency plans developed by private sector companies will inevitably concentrate on returning the organisation to its expected profit and revenue streams and not, for example, to seeing that a wider population is adequately fed, housed, able to communicate and have its health needs addressed.

As one looks more closely at government computing a further issue arises: much of its functionality and capability is not in government ownership – as we have seen, it is

outsourced. In some instances the parent of the outsourcing company may not even be in the same territory or jurisdiction as the government that uses its services.

Outsourcing operates on the basis of tightly negotiated Service Level Agreements. There are at least two potential problems. First, if the penalties for breach of the Agreement are limited to the value of the contract as opposed to the size of the consequential loss of the failure, the public purse will have to pick up the difference in the cost of full remedy. Second, the Service Level Agreement may only be designed to meet normal operational situations and not the heightened demands of an emergency. In an emergency a government would have to ask its outsourcer to provide additional facilities – and would have little alternative to paying whatever price the outsourcer requested.

Most governments, like the UK, have the facility to issue emergency decrees and take over such resources as are necessary. However although the power exists, one has to question how easy it would be to exercise. Who from the body of civil servants and military personnel would be able to "run" an electricity supply, an Internet service facility, a modern supermarket, and so on? At the moment there appears to be heavy reliance on the possibility that these private sector CNI facilities will perform in the national interest – and perhaps hope that proper compensation from central government funds will be forthcoming.

Public cybersecurity education programmes such as the UK's Get Safe Online (http://www.getsafeonline.org/) continue to be a worthwhile attempt to persuade users to take basic security precautions. However, these programmes can only complement, rather than substitute for, improving the default level of software and system security.

The UK's plans, in many respects much more advanced and sophisticated than those in some other OECD countries, cover government departments, local authorities, police and fire services, but not how to deal with private sector (UK Resilience, 2009). The US position, according to a July 2010 report from its General Accountability Office, appears to be rather more fractured. (GAO, 2010)

Policing and Counter-Fraud Responses

For the most part it is difficult to forecast a criminal act that could propagate into a full-scale global shock as opposed to a signifcant event with many victims. Nevertheless it is useful at this point to consider the role of policing. All, or nearly all countries have some form of specialist cybercrime unit. London's Metropolitan Police claim their original Computer Crime Unit was the first, in 1985. The FBI's Computer Analysis and Response Team, or CART, became operational in 1991. All such units share particular problems: it costs a great deal to train a cyber crime officer – and the training must constantly be renewed as computer and telecommunications technologies keep changing. Equipment needs constant upgrading. Staff must be both skilled detectives as well as resourceful users of relevant technology. Most police and quasi-police forces tend to reward management skills as opposed to ability in front-line crime-fighting, so that cyber crime officers are poorly paid in relation to their abilities – and after a short while are readily tempted into the private sector. (Sommer, 2004)

The vast majority of cybercrime investigations are complex, lengthy and expensive. For the heads of police forces, the budget for cybercrime investigation has to come from the same source as all their other work, which will include the fight against robbery, murders, narcotics trafficking and the more routine types of localised "street" crime which is nevertheless important to the communities they serve. Any significant cvbercrime is also highly likely to cross several national borders and jurisdictions, thus adding to the costs of investigation while making success less likely. Ksheti provides a cost-benefit analysis for cybercriminality. (2006)

As a result police activity in this arena cannot aim to bring to justice the vast majority of offenders. Instead it can, and does, embark on specific sample investigations where there is a reasonable prospect of success and with the aims of showing criminals that there is some risk in what they do and the public that cybercrime does not go wholly unpunished.

There seems little prospect for substantial increases in specialist police resource. However there are some low-cost measures which could improve police response. The first is to develop a promotion and reward scheme for specialist officers so that they are persuaded to stay longer in public service. Second, potential victims need to be educated about the issues of identifying, collecting, and preserving digital evidence – which is the raw material from which investigators and eventually the courts get results. Third, given the requirement for speedy action in an investigation before evidence disappears and given also that the arrangements for trans-national action are always going to be slow, much will depend on the extent to which key officers in different countries have been able to build strong informal relationships with their opposite numbers; important routes to these are via attendance at international conferences and vetted-access bulletin boards.

There is also significant value in the development of technologies which give early warning of frauds and intrusions and using these to alert officers to set traps to detect crimes and criminals in progress. These are discussed below.

But for the foreseeable future police investigatory action is likely to be limited to a small fraction of the total number of offences. For this reason, there continues to be a need for ongoing efforts to educate potential victims with awareness programs and in the use of preventative measures.

Research Responses

Traditional computer security research has operated on the "technological problem/technological solution model" and there is still a significant ongoing requirement for innovation in such areas as access control services, malware and intrusion detection systems, secure database design and cryptography. Much work is also needed in developing forensic and tracing tools and techniques. A further area is within intrusion and fraud detection. Both of these work on the basis of signatures of "bad" behaviour or heuristics of anomalies. The problem with these tools is how to set the alarm thresh-hold to avoid both false positives (alarming when there is no problem) and false negatives (failing to indicate that there is a problem).

The growing enthusiasm for cloud computing has brought further challenges including the need for sophisticated authentication and contingency plans against the possibility that a cloud supplier ceases to provide service or a failure of the communications link between users and supplier (NIST, 2010)But many researchers from a "hard computer science" background have come to appreciate the need to understand the social science dimensions. Computers are used by people within organisations and levels of information system security are achieved only by a fusion of technology and the ways in which people and organisations actually try to deploy them. Social science research is also helpful in understanding motivations and attitudes.

Among the disciplines of the social sciences, management, economics, criminology, psychology, anthropology and media studies have particular contributions. (Backhouse and Dhillon, 2000), (Anderson, Boehme, Clayton, Moore, 2008).

This cross-disciplinary approach has been manifest in a number of European Union 6th Framework projects on privacy, for example FIDIS (http://www.fidis.net/) and PRIME (https://www.prime-project.eu/) and also within the United Kingdom's main futurology

project, Foresight, which has included an exercise on *CyberTrust and Crime* (http://www.foresight.gov.uk/OurWork/CompletedProjects/CyberTrust/index.asp). There have also been established a series of annual workshops such as WEIS (Workshop on the Economics of Information Security - http://weis2010.econinfosec.org/)

There have also been a number of ad hoc workshops and meetings as well as more formal arrangements in the form of Knowledge Transfer Networks (https://cybersecuritychallenge.org.uk/ and http://www.cyber.st.dhs.gov/ are examples).

Many governments are already supporting this type of research in universities and high-tech companies, for example in the EU 7th Framework Programme. The US is developing a strategy to coordinate cybersecurity research across a number of federal agencies, so as to maximise its impact. It is also creating research "Grand Challenges" whose goal is to stimulate the deployment within 5-10 years of new technologies that would improve cybersecurity by "orders of magnitude".

An important feature of all these initiatives has been to compel researchers from very different backgrounds to appreciate each other's work, and in particular to understand their respective use of terminology.

Thus far the involvement of researchers in war studies and conflict resolution in these cross-disciplinary exercises has been relatively limited (and to date most of such activity has been in off-the-record seminars. As events involving the deployment of cyberweaponry increase in frequency and seriousness, a military element in research becomes more important. Research into how to evaluate intelligence – plausible but not fully verifiable information of potential strategic value – would also add value to such work.

Legal and Regulatory Approaches

The rapid development of computer and communications technology over the last 50 years has presented a challenge for national and international law. Acts such as computer manipulation and data theft often lay outside existing criminal offences. Law enforcement agencies sometimes lacked the powers to obtain evidence from Internet-connected systems, especially those outside their own jurisdiction. Many online criminal acts have a transnational dimension, but states' laws were frequently incompatible in their definitions of offences (United Nations, 2010a).

Given the rapid diffusion of the Internet since the late 1990s, states have taken a more coordinated approach to developing national and international legal responses to these problems. The Council of Europe, in cooperation with a number of non-European countries, developed an influential convention on cybercrime that came into force in 2004 – the Budapest Convention, The United Nations has developed model laws and provided other technical assistance to its members on reducing cybercrime and attacks on information systems. Regional organisations such as the Organisation of American States and APEC have coordinated their members' legal and regulatory responses. The European Union has gone furthest in developing binding laws on network and information security.

Council of Europe Convention on Cybercrime

The main international instrument intended to reduce cybersecurity risks is the Council of Europe's Convention on Cybercrime, which was agreed in 2001 and entered into force on 1 July 2004. The Convention contains common definitions for computer-related crimes such as system interference and computer-related fraud; procedures for preservation and production of digital evidence; and encourages international cooperation, with a "24/7

Network" of points of contact to provide immediate assistance and an annual meeting of signatories. It requires state parties to provide mutual assistance and to cooperate "to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."

The Convention has beenratified by 30 state parties, including the United States, and signed but not yet ratified by a further 17 states (including Canada, Japan and South Africa). It has also been used as a model for legislation in Latin America and several Middle Eastern nations. The most significant step to increase the effectiveness of the Convention would be the ratification of Russia – the source of a number of high-profile cyber-attacks and frauds – and the nation with the greatest number of Internet users, China (Brown, Edwards and Marsden, 2009).

However in April 2010 at the UN Crime Congress in Brazil, Russia China and a number of developing countries stated their opposition to the Cybercrime Convention largely over concerns that police might acquire powers to cross national boundaries without consent from the local authorities. (Ballard, 2010)

United Nations

The United Nations' International Telecommunication Union is in the final editing stages of the production of a "toolkit" to help its members develop their national cybercrime legislation (2009). This includes model legislative provisions based heavily on the Council of Europe Cybercrime Convention, as well as a comprehensive analysis of existing national and EU laws. This follows UN resolutions 55/63 and 56/121 on combating criminal misuse of information technologies and resolutions 57/239, 58/199 and 64/211 on protecting critical information infrastructures.

The UN has also been debating the need for a new global cybercrime treaty. At the recent Twelfth UN Congress on Crime Prevention and Criminal Justice, there was agreement that "cybercrime threatened economies, critical infrastructure, the credibility of institutions and social and cultural well-being." (United Nations, 2010b: 2). Russia has argued for a UN treaty that is more "respectful of borders" than the Council of Europe convention (The Economist, 2010). However, other states have responded that the convention provides an adequate legal framework and that effort should instead be concentrated on operational matters and capacity building in the developing world (United Nations, 2010b: 3—4).

European Union

The EU's legislative framework on network and information security is in two parts. In the former judicial and home affairs "third pillar", the Council passed a framework decision on attacks against information systems (2005). This closely follows the Cybercrime Convention in harmonising criminal offences and penalties related to access to and interference with information systems and data, and reinforces procedures for exchange of information. Three years after this measure, the Commission found that twenty member states had made "notable progress" in transposing the decision into national law, but that seven were still to take action (2008).

In the former single market "first pillar", the Council and Parliament very recently passed a major update of the legislation governing electronic communications. This adds a new Article to the framework directive (2009/140/EC) on security and integrity of networks and services. It strengthens network operators' obligations to ensure that appropriate technical and organisation security measures are taken, guarantee the continuity of supply of services and notify security breaches to national regulators.

Organization of American States

The OAS has since 1999 adopted a coordinating role on cybersecurity regulation. The member states' Ministers of Justice and Attorneys General group approved recommendations in 2000 and 2003 from an intergovernmental experts group that members facilitate broad and efficient cooperation on cybercrime; implement and consider acceding to the Council of Europe convention; and ensure that domestic agencies adapt to the shifting nature of cybercrime (ITU, 2009b: 106).

OECD

At the OECD Ministerial Meeting on the Future of the Internet Economy in Seoul South Korea in 2008, a *Recommendation of the Council on the Protection of Critical Information Infrastructures* was produced. It covers both national activities and ways of protecting infrastructures across borders. (OECD, 2008b)

National approaches

It is important to note that national law remains the focus of most government efforts to mitigate cybersecurity risk. These laws vary widely, although harmonisation is proceeding slowly as a result of agreements such as the Cybercrime Convention. The ITU has produced a detailed analysis of ten leading national laws:

Table 2 – Extract from provisions of leading cybercrime laws

Legal Provision	CoE	Australia	Canada	EU	Germany	Japan	Mexico	Singapore	UK[29]	US	India	China
Definitions				X					X[30]			
Definitions	X			X				X[31]	X[32]			X[33]
Computer System	X	X	X[34]	X				X[35]		X[36]	X[37]	
Computer Data	X	X	X[38]	X	X[39]			X[40]	X		X[41]	
Service Provider	X	X						see[42]	X		X[43]	
Traffic Data	X	X	X[44]	X				see[45]	X	X		
Substantive Criminal Law												
Illegal Access	X	X[46]	X[47]	X	X[48]	X[49]	X	X[50]	X	X[51]	X[52]	X[53]

Source: ITU (2009: 37-44)

There are obvious sensitivities over national sovereignty in areas of defence and criminal law enforcement. Even when adequate legal provisions are in place, it is not always the case that they are effectively enforced. Political considerations play a significant role. James Lewis commented:

> *"We should not forget that many of the countries that are havens for cybercrime have invested billions in domestic communications monitoring to supplement an already extensive set of police tools for political control. The notion that a cybercriminal in one of these countries operates without the knowledge and thus tacit consent of the government is difficult to accept. A hacker who turned his sights from Tallinn to the Kremlin would have only hours before his service were cut off, his door was smashed down and his computer confiscated... The political environment in which the most advanced cybercriminals exist militates against them becoming mercenaries for many terrorist groups without the consent of their host." (2009: 8)*

International regulatory and private-sector cooperation

While much of the Internet and related infrastructure is operated privately, the mitigation of cybersecurity risk has a public good element that requires the involvement of governments. As the House of Lords EU Committee commented: "Not only do governments themselves

believe that Critical National Infrastructure is a matter for them, but in times of crisis, citizens agree with that analysis" (2010: 23). There are a number of intergovernmental efforts on cybersecurity, all of which involve the participation of industry and academic experts and some of which further include civil society organisations that are concerned to ensure the protection of fundamental rights.

Earlier this decade, the OECD developed nine guideline principles to encourage a "culture of security" among governments, businesses and users. These include awareness building; collective responsibility and response; the consideration of ethics and democratic values; broad-based risk assessment; and the incorporation of security in system design, implementation and ongoing management (2002). The United Nations, European Union Council, APEC and ASEM have all made use of the principles. The OECD maintains a web site for governments to share policies and best practice, and as noted above recently produced a Council recommendation on Critical Information Infrastructures (OECD, 2008b)

The International Telecommunication Union (ITU) runs a number of activities on cybersecurity for its 191 member states, within a mandate from the UN's World Summit on the Information Society. The ITU has produced guides for developing countries on cybersecurity (2009) and cybercrime (2009b); a toolkit for botnet mitigation; and a national critical information infrastructure protection self-assessment tool (2009c). With ETH Zurich it has produced a generic framework for critical information infrastructure protection (2007). It collaborates with the International Multilateral Partnership Against Cyber Threats to operate an early warning system and a secure electronic collaboration platform for coordination of responses to crisis situations. It has hosted a series of Regional Cybersecurity Forums since 2004.

In 1998 the Group of Eight (G8) ministerial meeting approved ten principles and an action plan to combat high-tech crime. A G8 subgroup on high-tech crime has since added protection of critical information infrastructures to its mission, creating a network of 24-hour points of contact in nearly 50 countries, producing best practice guides on international requests for assistance and running conferences and training courses (US Department of Justice, 2004). The G8 Justice and Interior Ministers adopted updated principles in 2003.

Interpol has set up regional expert groups on Information Technology Crime in Europe, Africa, Asia-Pacific and Latin America. These groups hold regular meetings and training workshops for representatives from national computer crime units, and produce documents such as an IT Crime Investigation Manual. The European group runs a rapid information exchange system with national contact points in over 100 countries, and is currently planning a project on botnets and malicious software (Interpol, 2009).

Since the 2007 cyber-attacks on Estonia, NATO has established a Cyber Defence Management Authority (CDMA) to protect NATO's own information systems and provide assistance to allies on request; and, as noted above, has established a Centre of Excellence in the Estonian capital Tallinn. It is exploring options for its members to cooperate further on cyber-defence (NATO, 2008). The UK House of Lords has urged NATO to work closely with the EU "to achieve cooperation rather than duplication" (2010: 26).

Through its Project on Cybercrime, the Council of Europe provides ongoing assistance to countries that wish to accede to and implement the Cybercrime Convention. This has included organising workshops jointly with national governments and intergovernmental groups such as the Organisation of American States. The Council has also developed guidelines for cooperation between law enforcement agencies and Internet Service Providers, which suggest mechanisms for information exchange, sharing of best practice, training, effective procedures and the development of comprehensive criminal compliance programmes (Council of Europe, 2008).

Within the European Union, the European Network and Information Security Agency (ENISA) was set up in 2004 as a centre of excellence to advise the European Commission and to allow the 27 member states to exchange information and best practice. ENISA's

mandate currently excludes public security and defence, but this may change as the EU's overall institutional framework adjusts as a consequence of the Treaty of Lisbon. In a recent communication, the European Commission has proposed that this coordination be strengthened; that a pan-European multi-stakeholder governance framework be developed; and that incident response and international cooperation be improved (2009). In response, ENISA is planning a cross-EU exercise in November 2010 to practice the response to a large-scale network security incident. The Commission is also examining the designation of certain information infrastructures under the Council Directive on European Critical Infrastructures, although this cannot occur until the Directive is revised following a review planned for 2012 (2008).

In the Asia-Pacific region, APEC has set up a Security and Prosperity Steering Group to coordinate its members' cybersecurity work. It has recently run workshops on submarine cable protection and cybersecurity awareness, and also undertakes work on ICT in disaster preparedness and recovery, cybercrime prevention and the development of Computer Emergency Response Teams. APEC leaders have committed to enact comprehensive cybercrime laws consistent with the Cybercrime Convention; create national cybercrime units and points of contact; and establish institutions to exchange threat and vulnerability assessment (APEC, 2002).

One obstacle to full multi-stakeholder involvement in cybersecurity efforts is the sometimes-sensitive nature of the operational information required to make an accurate assessment of current risks. Former UK Security Minister Lord West told a recent House of Lords EU Committee inquiry: "We need to develop mechanisms where we are talking to a much broader range of the innovative entrepreneurial businesses in the UK, but it is difficult to see quite how we can do that and still maintain this trusted environment, and that is the challenge we have" (2010: 24). The British Computer Society complained: "In the security field, public-private partnerships tend to be talking shops rather than joint ventures. They are useful for sharing best practices but by themselves are unlikely to drive through the required levels of change" (2010: 25). However, the Committee concluded that this difficulty should be overcome, concluding: "the involvement of Internet entrepreneurs in the formulation of Government policy is as yet at best superficial. Both the Government and the (European) Commission seem to think that it is for the private sector to come forward. We think that, on the contrary, it is for the public sector to take the initiative and to offer to experienced Internet entrepreneurs a real say in how public private partnerships are best developed." (2010: 25)

Some countries (such as the United States) have updated their legislation in line with the Council of Europe Convention on Cybercrime, developed comprehensive national strategies and programmes to address risks across the public and private sector, and appropriately supported prosecutorial efforts and networks of Computer Emergency Response Teams (CERTs) across key sectors. Others (such as some eastern European Union Member States) have failed to fully implement standards such as the Council of Europe's Cybercrime Convention, and in some cases even lack institutions such as a national CERT to respond to computer security incidents. The main reason that the 2007 cyber-attacks on Estonia had a significant impact was that the country had become highly dependent upon information infrastructures without having made a concomitant investment in cybersecurity activities (House of Lords EU Committee, 2010: 10).

CERTs and FIRST

Shortly after the Internet worm of 1988, the first Computer Emergency Response Team (CERT) was set up at Carnegie Mellon University. By 2000 a number of other CERTs had been set up and FIRST (Forum for Internet Response and Security Teams) was set up in 1990. The aim is to share information, best practices and tools and to have confidential routes to identifying and limiting the spread of computer-related risks. Originally FIRST was almost exclusively populated by skilled Internet technicians but in 2005 corporate executives were given their own specialist program. CERTs are essentially civilian and non-military. Today most countries have an official government CERT as well as CERTs specific to individual organisations and industries. An alternative name for CERT is CSIRT – Computer Security Incident Response Team.

One of the benefits of the FIRST meetings is that, in addition to spending time analysing potential future problems, computer security engineers in different countries get to meet each other and build informal relationships of trust. Such social contacts can, in an emergency, help resolve problems more quickly than via the official formal structures.

Many OECD Member countries are also taking longer-term measures to reduce societal cybersecurity risk. These include funding for security education and research; sponsoring the creation of security standards; educating businesses and individuals about the issue; resourcing cyber forensics and early-warning activities; and encouraging information sharing within and between the public and private sectors (Libicki, 2009: 129; US Executive Office of the President, 2010; UK Cabinet Office, 2009

Technology's role in emergency response

Recovery from most types of disaster is dependent on linked computer and communications facilities, many of them in the private sector. Commonly occurring disasters include earthquakes; human and animal pandemics; large-scale floods; the escape of noxious substances via air and water; the collapse of an essential route, such as a key bridge, harbour or road inter-change; and a train, plane or ship disaster. They also include the aftermath of successful terrorist attack, which in the worst situations could include chemical, biological or radiological weaponry.

The critical role of ICT is apparent in any emergencies as identified by the UK Civil Contingency Secretariat's "capability work streams". In the table below we have taken the structure detailed by the secretariat and added a commentary on the role of technology. The position is not very different in many other OECD countries:

The Four Structural Workstreams	***Technology needed***
1. Central Response	*To collect detailed information about the scope of the catastrophe, to make most use of and prioritise the work of available resources for mitigation and recover; to communicate with victims and the public at large*
2. Regional Response	
3. Local Response	
4. Resilient Telecommunications	
The Ten Functional Workstreams	
5. Chemical, Biological, Radiological and Nuclear (CBRN) Resilience	*To map extent of effects, specialist clear-up, communication to hospitals etc, communication with public*

6. Infectious Diseases – Human	*To map extent of effects, decisions about restricting movement of people, communication to health care, hospitals etc, communication with public*
7. Infectious Diseases - Animal and Plant	*To map extent of effects, decisions about restricting movement of animals, plants etc, communication to health care, hospitals, farmers and agribusiness etc, communication with public*
8. Mass Casualties	*To map extent of effects, communication to hospitals etc, communication with public*
9. Evacuation and Shelter	*To map extent of effects, communication to hospitals, social services, voluntary organisations etc, communication with public*
10. Warning and Informing the Public	*Communication with public*
11. Mass Fatalities	*To map extent of effects, communication to hospitals etc, communication with public*
12. Humanitarian Assistance in Emergencies	*To map extent of effects, communication to hospitals etc, communication with public*
13. Flooding	*To map extent of effects, communication to hospitals etc, communication with public*
14. Recovery	*To map extent of effects, communication with public, social services, etc*
<u>The Six Essential Services Workstreams</u>	
15. Health Services	*To collect and analyse data; to provide data to professionals and the public; to provide support for industry-specific infrastructures*
16. Food and Water	
17. Transport	
18. Energy	
19. Telecommunications and Postal Services	
20. Financial Services	*The industry deals less and less with physical cash and physical documents; without ICT for communications, secure storage and robust authentication, the only transactions that are possible will rely on barter, gold and cash*

Because the Internet is now a key channel for governments to provide information to the public, it will in future play an important role in dampening all kinds of systemic risks. The provision of advice and accurate up-to-date situational information can have a significant calming effect, and help to shape public responses in a way that will reduce pressure on healthcare and other critical services in an emergency. This was a key response of many governments to the 2008 financial crisis and the 2009 swine flu pandemic. Ensuring the resilience and high availability of such information services should therefore be a key part of governments' civil contingency plans.

The availability of communications services that are increasingly based on Internet technology can also be critical in emergency situations. Natural disasters and terrorist attacks often cause local phone networks to be swamped as those in the affected areas attempt to communicate with emergency services and with friends and family. For the example, the 1995 Kobe earthquake in Japan saw telecommunications traffic rise to 50 times its usual peak volume (Noam and Sato, 1995: 596). The resulting congestion can damage the ability of emergency responders to communicate with each other and with bases to coordinate their actions.

Telephone networks commonly include the ability for authorised officials to gain priority "dial tone" and make calls when a system is overloaded (Carlberg et al., 2003). Emergency services should include the provision and regular training in use of such services in their disaster response plans, while network operators ensure they cannot be accessed or abused by unauthorised users. The Kobe earthquake also demonstrated the utility of open online information-sharing mechanisms for emergency workers, survivors and volunteers. Information about the state of neighbourhoods and individuals was shared using a bulletin-board system that bypassed congested "official" communication channels (Noam and Sato, 1995: 597—598). Similar tools have been used in more recent disasters, particularly now that media such as blogs, Twitter and social network sites are so widespread. An interesting development has been Ushahidi (www.ushahidi.com) which emerged in Kenya during a time of crisis but has developed into a more universal vehicle of crowd-sourcing emergency information-sharing providing, among other things, interactive maps of developing and on-going disasters. But it only works if there is good Internet connectivity in the affected regions.

Accurate and trustworthy cybersecurity risk assessments will play an important role in persuading government departments, legislators and the private sector to appropriately resource investment in the resilience of critical systems. Many cybersecurity risks are not as easy to understand or newsworthy as the Y2K risks that energised public and private sector responses during the 1990s (Mussington, 2002). Independent forums that brought together government, industry and academia proved a useful mechanism in the development and dissemination of trusted information on Y2K (Quigley, 2004: 815—816). Governments might consider co-sponsoring similar efforts for cybersecurity, especially given the conflict of interest inherent in having significant input into public sector information security efforts from national signals intelligence agencies, as in the United States and United Kingdom (US Executive Office of the President, 2010; Cabinet Office, 2009).

Many of the tools that give rise to systemic cybersecurity risks rely on the availability of a large pool of insecure Internet-connected personal computers. Educational materials to help train Internet users in improving their own system security can in the longer term reduce the number of such machines. These are being produced in a number of OECD Member states by government agencies and public-private partnerships, including the US Department of Homeland Security Computer Emergency Response Team and the UK's Get Safe Online programme.

One particular concern is the cascade/system overload scenario – that the specifications of individual systems are not strong enough to cope with levels of traffic that will be required in an emergency. Moreover if government seems unable to cope or provide information about how it proposes to cope, this may trigger unrest among the public at large, as they take a series of actions to protect themselves against supposed shortages.

Appendix 2 to this Report illustrates what could happen if there is failure of critical cyber resources during a more conventional type of disaster.

It seems unlikely that the Internet as a whole could be made to collapse. But there are two scenarios that governments need to prepare for:

- Localised but significant failure of Internet service in all or part of their territory, possibly occasioned by failure at a major Internet Exchange in turn caused by fire, flood, bomb, failure of electricity supply. Such a failure would disconnect the population as a whole from online government guidance and information and would also inhibit the role of emergency responders.
- Overload of web servers supplying information and services to the public and gathering information from the public about its needs.

The United States Government Accountability Office, analysing the implications of an expected influenza pandemic in 2009, commented:

> *Increased use of the Internet by students, teleworkers, and others during a severe pandemic is expected to create congestion in Internet access networks that serve metropolitan and other residential neighborhoods. For example, localities may choose to close schools and these students, confined at home, will likely look to the Internet for entertainment, including downloading or "streaming" videos, playing online games, and engaging in potential activities that may consume large amounts of network capacity (bandwidth). Additionally, people who are ill or are caring for sick family members will be at home and could add to Internet traffic by accessing online sites for health, news, and other information. This increased and sustained recreational or other use by the general public during a pandemic outbreak will likely lead to a significant increase in traffic on residential networks. If theaters, sporting events, or other public gatherings are curtailed, use of the Internet for entertainment and information is likely to increase even more. Furthermore, the government has recommended teleworking as an option for businesses to keep operations running during a pandemic. Thus, many workers will be working from home, competing with recreational and other users for bandwidth.*
>
> *According to a DHS study and Internet providers, this additional pandemic-related traffic is likely to exceed the capacity of Internet providers' network infrastructure in metropolitan residential Internet access networks.15 Residential Internet users typically connect their computers to their Internet service providers' network through a modem or similar Internet access device. These Internet access devices route home users' traffic to a network device that aggregates it with that of other users before forwarding it to the other parts of the provider's network and its ultimate destination on the Internet (GAO, 2009; Rivera, 2009).*

Conclusions and Recommendations

The remarkable speed of change in the cyberworld – hardware, software, interconnectivity – and the ever-new social, cultural and economic structures being created – makes it essential that there is frequent re-assessment of the associated patterns of threat. Unfortunately too many published assessments have favoured sensationalism over careful analysis. To understand potential problems, particularly large-scale ones, requires more than simply identifying potential vulnerabilities. An examination of all the necessary elements of a crime, attack or catastrophe is required, in addition to consideration of the processes of prevention, mitigation and recovery. Risks have to be properly assessed and then managed.

A critical feature of any worthwhile analysis is discipline in the use of language. Cyber espionage is not "a few clicks away" from cyberwar, it is spying which is not normally thought of as "war". By the same token a short-term attack by hacktivists is not cyberwar either but is best understood as a form of public protest.

The two appendices indicate that, contrary to many assertions and on present information, few single foreseeable cyber-related events have the capacity to propagate onwards and become a full-scale "global shock". One would have to contemplate a hitherto unknown fundamental flaw in the critical technical protocols of the Internet and over which agreement for remedy could not be quickly reached. Or a succession of multiple cyber-attacks by perpetrators of great skill and determination who did not care if their actions cascaded beyond their control and consumed both them and the constituency from which they came. Or an exceptionally strong solar flare coupled with a failure adequately to protect key components.

This does not mean that individual cyber-related events cannot generate a great deal of harm and financial suffering; indeed there are many examples where this has already happened. What should concern policy makers are combinations of events – two different cyber-events occurring at the same time, or a cyber-event taking place during some other form of disaster or attack.. In that eventuality, "perfect storm" conditions could exist.

A pure cyberwar, that is one fought solely with cyber-weapons, is unlikely. On the other hand in nearly all future wars as well as the skirmishes that precede them policymakers must expect the use of cyberweaponry as a disrupter or force multiplier, deployed in conjunction with more conventional kinetic weaponry. Cyberweaponry of many degrees of force will also be increasingly deployed and with increasing effect by ideological activists of all persuasions and interests.

Our main reasons for reaching these conclusions are: that the Internet was designed from the start to be robust so that failures in one part are routed around; that in most cyber-events there is no loss of physical resource; that historically, solutions to discovered flaws in software and operating systems and/or the emergence of new forms of malware have been found and made available within a few days; that few single DDoS attacks have lasted more than a day; that many government departments and major businesses and organisations have ICT-related back-up and contingency plans; and many of the networks transmitting the most important data, for example about world financial transactions, are not connected to the Internet, use specialised protocols and equipment, and have reasonably strong levels of access control. Any successful compromise requires insider knowledge – and the response to that is better vetting procedures, not specialist technology.

There is also a further limitation on anyone planning an all-out cyberwar: given the levels of mutual dependency and interconnectedness, outcomes from the deployment of a succession of large numbers of powerful attacks are very uncertain; self-damage is a real possibility.

Although it is obviously rash to make predictions beyond a very few years about the evolution of cyberspace, there seems little prospect that security issues will diminish. The population of Internet users will continue to grow, newer arrivals will initially be less skilled in computer usage and hence more vulnerable to security threats. There will be even more computers connected to the Internet, both to become victims of attack and to provide zombie vehicles by which other computers will be attacked. Computer hardware and software will become even more complex and this will make it more difficult to debug flaws. Cloud computing, which has potential benefits to users in terms of instant availability and resource and information sharing, also potentially creates significant security vulnerabilities: large-scale cloud facilities without sufficient redundancy could be a single point of failure in terms of availability and confidentiality. Marketing and revenue imperatives will continue to prompt vendors to release products with less than exhaustive testing.

Businesses and governments will continue to desire the efficiency savings that computers present and in particular will want to speed the process by which as many transactions with customers, counter-parties and citizens as possible are mediated over the web. But as this process goes on, so will the parallel activities of closing down local offices and shedding staff, so that if the web-based service fails, there is no fall back. At the same time the cost-savings of just-in-time manufacture and retail distribution will also continue to be attractive, as will the opportunities to manage large grids of electricity, water and fuel supply via the Internet.

Preventative and detective security technologies will not provide protection against all the threats; considerable effort will be needed to mitigate and recover from losses.

In terms of cyber attacks the one overwhelming characteristic is that most of the time it will be impossible for victims to ascertain the identity of the attacker – the problem of attribution. This means that a defence doctrine based on deterrence will not work. In effect, one has to look to resilience so that when attacks succeed, societies can absorb and recover.

Whether or not a single cybersecurity event can develop into a global shock, the policy imperatives for governments to mitigate the impact of such events on their own citizens remain the same.

National Strategies

The most immediately effective action that governments can take is to improve the security standards of their own critical information systems. While classified networks are generally run to very high standards, many other government systems are run using (sometimes out-of-date) commercial software that is not configured appropriately. Internet connectivity is often purchased with fewer guarantees of availability than that available in traditional telephony networks. Monitoring of networks for signs of intrusions is done in a patchy and uncoordinated way. Responsibility for cyber security is often spread across business, law enforcement, the military, defence and intelligence agencies with little effective collaboration. Too often systems are procured without the precaution of a thorough and independent security audit.

By procuring and operating more secure systems, governments will reduce the risk of exploitation and failure of their own critical services. They will also incentivise software companies, Internet Service Providers and other companies to create more secure products that can also be sold to the private sector. It remains the case that leading software companies release products before thorough testing has taken place, hoping that errors can be rectified as they emerge by the rapid provision of patches. National governments as

large-scale purchasers are in a strong position to refuse to buy new software and operating system products until they can be convinced that thorough testing has taken place. Government agencies face considerable pressure to reduce the costs of their large-scale information systems. Outsourcing and the use of cloud computing is likely to become increasingly popular as a result over the next decade. Agencies need to carefully consider the implications for the resilience of the services they provide, identifying any new inter-dependencies that result and how they would deal with catastrophic failure of third-party services. Contracts and Service Level Agreements need to include provisions on availability and liability for security breaches, as well as the geographic location of sensitive data and the level of access of third-party staff.

Governments need to proceed cautiously when planning citizen-to-government and business-to-government services which will become available solely via the web. Either such services must feature considerable internal resilience or there must be some alternative route by which the most important traffic and transactions can still take place.

Military Responses

Military agencies have the strongest requirement both to secure their own information systems, and to understand the types of cyberattacks that might be launched against them during armed conflict. Improving system defence and resilience should be the core focus of military strategy in this domain. Because of the difficulties of attribution of attacks, doctrines of deterrence are unlikely to be effective.

It is not too difficult for nation states to set up covert cyber attack units. Any agency that researches, for defensive purposes, the nature of cyberattacks has all the knowledge needed to originate attacks and disguise the fact that they are doing so. Moreover, unlike the situation with most forms of novel kinetic attack, little capital investment in terms of new planes, ships, tanks, guns etc is required, nearly all cyberattacks use hijacked innocent zombie machines as vectors. All that is required is a modest amount of research, code writing, and the political decision to deploy.

One possible response to this inevitable proliferation of national cyberattack units could be a new international treaty on the lines of the Nuclear Non-Proliferation Treaty of 1970 with its 189 signatories, the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction of 1975 and the similar Chemical Weapons Convention of 1993. However a key feature of this latter treaty is the ability of signatories to arrange inspection of each others' facilities in order to check for compliance. Given the nature of cyberweaponry and its deployment reliable inspection is almost impossible to achieve.A better deterrent to state-sponsored cyberattack is awareness that such attacks are often uncertain in their effects and eventual outcome; it is this uncertainty which has thus far limited the deployment of biological weapons in particular.

Civilian Impact

The most serious cyber security failures, accidental and deliberate, can impact the population as a whole. OECD countries seem to vary in their attitudes about the extent of the obligation of their governments to provide protection and contingency plans. This is a role for civilian agencies rather than the military and such agencies will need to know how to work with the private sector, a matter we explore below. Some countries are criticized as viewing cybersecurity from a military perspective, whereas others approach it as matter of civil protection, bringing support from across ministries and government agencies. Officials will need, if they are not doing so already, to plot out the dependencies of key

central government and critical infrastructure systems. They will need to identify points at which computer and communications facilities may become overloaded during catastrophes and arrange for the provision of extra resource and resilience. They will also need to create contingency plans should large important systems fail. A further role is horizon-scanning for future threats arising from changes in the broad cyber world.

Public Private Partnerships

In the medium term it is extremely unlikely that OECD Member states will reverse the trend for significant parts of Critical Infrastructures to be operated by private companies. This rules out direct state control of the security of communications infrastructures and the information systems upon which power and water utilities, healthcare providers and others are critically dependent. Private operators have incentives to maintain continuity of service to their customers, but without some government intervention they may not be willing to commit resources to protecting such wider interests of society as public confidence promoted by the general availability of shelter, electricity and gas, and telecommunications.

Governments can facilitate partnerships with critical infrastructure operators to share best practice, threat updates and analysis, and data on attacks. As a last resort after a catastrophic event, government agencies may need to take direct control over the operation of critical information infrastructures using emergency powers. However, agencies will only be able to manage such complex, highly technological systems with close industry assistance. Action taken before such events to increase infrastructural resilience is highly preferable to more direct intervention after a disaster has occurred. But here greater clarity and candour is needed over the precise form of "public private partnerships" if the phrase is to be more than a description of an aspiration, and to avoid arrangements collapsing under the pressure of real events. One route to exploring these issues is to devise war games specifically designed to explore the tensions between government and private sector entities, as opposed to the more usual aim of determining the overall level of damage likely to be sustained in a particular scenario.

Governments can use legislation, licensing and regulation to impose standards for security and resilience upon operators of Critical Infrastructure. This should become a core concern for regulatory agencies in the water, power, telecommunications, financial services and healthcare sectors. Just as has become common in the financial industries, regulators should conduct regular "stress test" exercises to measure vulnerabilities and ensure the resilience of infrastructure in the face of attack.

International Strategies

International cooperation is one key to reducing cybersecurity risks. Attacks on systems connected to the public Internet can originate from anywhere on that network. Vulnerabilities in software developed in one country and installed in a second can be exploited remotely from a third. Failures in critical information infrastructures in one nation can cascade into dependent systems elsewhere. Governments and the private sector need to coordinate their efforts to enhance cybersecurity levels, develop safe and trusted methods for information sharing about vulnerabilities, block and deter attacks, and improve the resilience of critical infrastructure.

Although many international bodies have issued statements of principles of mutual support and protection, there is no substantive international governance mechanism for resolving cyber-related crises other than the engineer-dominated FIRST/CERT structure.

The main improvements that could be made would be to further increase the number of parties to the Cybercrime Convention, and to strengthen mechanisms for global cooperation and capacity building. It would be particularly helpful for countries with very large numbers of Internet users, such as Russia and China, to ratify the Cybercrime Convention. That may

require some flexibility from existing parties to meet concerns by Russia and others over sovereignty. The United Nation's Internet Governance Forum already brings together stakeholders from the public and private sector as well as civil society groups from around the world, and has actively considered security issues. If the UN decides to continue the existence of the forum, it would be an ideal venue for further global debate.

Possible New Technical Measures

Several technical measures could be pursued to improve cybersecurity. Further exploration of ways to strengthen the Internet's infrastructure is needed. One recent example has been the deployment of DNSSEC which strengthens the root domain servers by providing digitally signed authentication of DNS information. Similar work is required to strengthen the Border Gateway Protocol which controls ISP to ISP traffic routing. The difficulty is that changes to Internet protocols occur by a process of agreement and consent and in addition to the actual technical discussions, there is often a debate between freedom and control.

A second proposal is to seek to force each person to have their own, firm Internet Identity. Some policy-makers hope that this can be achieved via the move to IP v 6, a process which is already necessary as the existing IP address system is now more-or-less full. The problems with such proposals are: that enrolment, the process by which a real person is linked (or "bound") is complex, that there are legitimate circumstances where people may wish to act anonymously, and that it would still be possible for a perpetrator to take over a person'scomputer and hence steal their identity.

A third possible technical measure is sometimes referred to as the "Internet Off- Switch", a version of which was proposed in the United States Senate in June 2010. In the very simplest sense the Internet cannot really be switched off because it has no centre. On the other hand, at nation state level it is possible to envisage a situation where traffic passing through critical switches is, in an emergency, filtered and shaped. However there are formidable problems in implementing a prioritisation policy. For example, in most emergencies you would want to give priority to doctors, but most doctors and their surgeries use the same downstream Internet facilities as the bulk of the population and there would be no easy way to identify them. Localised Internet switch-off is likely to have significant unwanted consequences.

Users continue to struggle with badly designed security mechanisms that get in the way of their tasks and goals. Quite understandably, many users' response is to circumvent or switch off entirely such controls.

Research

The rapid ongoing evolution of computing and communications technology makes it difficult for governments to maintain a clear and comprehensive understanding of cybersecurity risks. There is a considerable difference between the effects of "possible" and "likely" scenarios. Much more reliable and comparable data is needed on the economic and social impact of attacks. Regulators need a better idea of the inter-dependencies of systems supporting critical national infrastructure, as well as an up-to-date understanding of the motivations and capabilities of potential attackers. Policymakers need to be able to identify and remove incentives that are causing market actors to under-protect systems. They also need the capability to horizon-scan for new threats, and to understand the likely long-term

direction of technological development. This research will need to draw on both computer science and social science disciplines such as management, economics, criminology and anthropology. Within computer science itself, more work is required to develop better methods of testing software and hardware for bugs; all too often these flaws are converted into the exploits deployed by cyber criminals and others.

Improvements are also urgently required in the security quality and capabilities of software and communications systems. The managers of critical information systems need better facilities to detect and block attempts to breach security controls. Law enforcement agencies need new tools to track the originators of such attacks. Users need much more user-friendly software that enables them to carry out their day-to-day activities in a secure way.

The scenario-based risk assessment that this study has used in its two major appendices has the benefit of identifying initial triggering events and the various elements that might lead to propagation. But it also helps identify what specific preventative and loss mitigation measures are required, and where they should be placed.

The possibility of an exceptionally energetic solar flare needs to be taken seriously. The computerised units that are most vulnerable are those that cannot easily be taken off-line because they provide an essential always-running service and which have cables and antenna-like devices which draw the energy towards sensitive internal components. Research is required to identify such units and to build cost-effective devices to limit the impact of the unwanted dangerous electro-magnetic radiation.

Further work is also needed to strengthen the investigative resources of the police and similar agencies. Particular areas are: better tools for tracing and forensic analysis, easier to deploy techniques for capturing evidence and more accurate systems for detecting intrusions and attempts at fraud which can then be acted on.

Education

Governments, regulators and the operators of Critical Infrastructure will all need a stream of well-trained staff to run their cybersecurity efforts. The US has recently concluded that there "are not enough cybersecurity experts within the Federal Government or private sector" and that a national effort is needed to develop a "technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees". The UK too has launched a Cyber Security Challenge to recruit new talent. Among other things it features a competition the reward for which is high quality training. The US is also expanding cyber counterintelligence education efforts across the government.

There will never be enough policing resource to investigate all computer-related criminal attacks. The public will have to continue to learn to protect itself – and that suggests a strong argument for some public funding for relevant user education. .

Many cyber attacks depend on the use of compromised personal computers. Improved public understanding of security therefore benefits governments as well as individuals and makes the task of the attacker more difficult.

As with other forms of hazard where large sections of the public are likely to be affected, education is needed to help citizens appreciate that while the risks and the damage from them cannot be eliminated, they can very often be managed.

Appendix 1

The table illustrates some typical feasible cyber-related events and analyses them for likelihood, duration and propagation. The purpose is not to make precise forecasts or to produce an exhaustive list, but to build an understanding of some of the key mechanisms and risk factors. Some of the events described as a "failure" or a "compromise" are neutral as to whether the cause is deliberate or accidental – the focus is on effects. Not all boxes are filled where the events are unlikely to occur.

Event	Triggers / Likelihood of Occurrence / Ease of Implementation	Local / Short-Term Impact	Likely Duration / Recovery factors - immediate	Propagation	Recovery factors – Longer Term (if applicable)	Potential for Global Impact
Fundamental compromise of Internet infrastructure	*The Internet was designed from inception to be resilient physically and logically. Local failures are routed around. Global failure would require a hard-to-fix vulnerability in a large fraction of central routers and domain name servers and/or compromise of the Border Gateway Protocol. There has to be not only a flaw but the means and motive to exploit it.* *Self inflicted harm that would occur to a perpetrator is a factor against the probability of one trying to accomplish this*	*If successfully exploited, services such as the world wide web and email would cease to work. Depending on the nature of the flaw it might be possible to communicate using IP addresses. However this would only be open to technologically sophisticated users and would rely on access to a reliable directory.*	*CERTs are in existence for precisely this eventuality but consensual agreement may be needed for full remedy.*	*Could be considerable as many Internet-based services are essential to government, businesses and organisations.*	*If a technical fix is found quickly there may be some loss of confidence in Internet-based services, but otherwise a full recovery would be achievable,*	*Yes, if successf ul*

Large-scale solar flare	*Solar Storms and Coronal Mass Injections occur potentially every 11 years. Actual events are difficult to predict without extensive monitoring, which does not currently exist. Satellite and cellular base stations may be affected directly and powerlines subjected to geomagnetically induced currents*	*A geomagnetic storm induced a 9-hour blackout in Quebec in 1989 affecting several million people and a Japanese satellite was permanently damaged in 2003. Actual damage may depend on which part of the earth is facing the sun at the time*	*The peak events often last only a few hours, so that the issue is the amount of induced physical damage and the extent to which key components had been protected. Networks and grids might be able to route around local failures and recover after a few hours. If satellites are affected some re-routing to alternative satellites may be possible unless the flare was very powerful*	*Loss of power from a electricity grid will kill industry, transport and many other critical services for the duration. Loss of communications capability will have a similar effect, but which will be difficult to remedy until alternative routes are established*	*In a very large event there may be significant physical damage to key nodes, which would need to be replaced. Spares may not be readily available and replacement satellites might require a lead time of several months*	*Yes, if very large scale.*

Zero day fundamental flaw in popular operating system	*Most likely candidate is a flaw in the Windows kernel, the central part of the Operating System. However the flaw would have to be triggered by some exploit, which in turn would have to be delivered to each computer*	*PCs where the exploit has arrived would cease to work or would cease to be reliable. Those with unaffected computers would need to avoid any connectivity – e.g. email or the world wide web, depending on the transmission method/route of the exploit.*	*News of the exploit would appear within 24-48 hours, together with initial (and probably partial) advice on evasion. A fuller remedy might take 7 or more days and would be in the form of a patch. Advice would need to be disseminated about acquiring and applying the patch safely.*	*Some computer systems providing real-time services (for example in banking, retail and industrial process control) would have to be curtailed pending provision of a safe patch. These would then have further economic impact*		*Low*
Large-scale failure at telecommunications service provider	*There are a handful of very large telecommunications providers such as BT, Alcatel, and Vodafone with global significance via their ownership of cables and switches. A software failure might occur when a new version of critical software is loaded across their networks, or internal sabotage.*	*Loss of telephone and Internet service to customers of failing telecom provider. Other providers unlikely to be affected other than for inter-connects and temporarily higher traffic re-routed from affected network*	*Recovery likely to occur via reverting to previously installed software; then gradual fixes of failed software. a few hours?*	*Customers who had no second supplier would be non-functioning for the duration. This could include CI services – but these ought to have contingency plans*		*Low and short-term*

Large-scale failure of critical network facility: cable, landing, satellite link or switch	*Bomb, fire, flood, earthquake, severed cable. All these have occurred. Could be the result either of accident or deliberate action. Also possibly compromised switch hardware*	*Loss of local service. Telecommunications including Internet will re-route automatically but there will be a loss of throughput.*	*Could be several days or even weeks, depending on severity. ISPs may need to consider limiting bandwidth-intense applications like video streaming. Telephone companies may need to favour priority customers*	*Customers who had no second supplier would be at very reduced functionality for the duration. This could include CII services – but these ought to have contingency plans which include obtaining priority from ISPs and CSPs*	*After several days or weeks, recovery will have been achieved*	*Low and short-term*
Large-scale failure of electricity supply	*Flood, fire, earthquake, bomb, High demand due to very hot or very cold weather. Poor equipment maintenance. Failure of grid management facilities*	*Loss of service to customers – local and semi-local. Loss of CII facilities which lack a back-up generator or similar*	*Electricity is usually supplied via a grid so that some service can be restored in hours. More remote locations may have to wait days, but not much longer.*	*Electricity is used to service supply of water, oil, hospitals, retail food stores. When a local supply fails, the grid tries to demand service from adjacent facilities; if these become overloaded a cascade of failures may follow*	*None of the existing power outages of potential continental significance have lasted more than 24 hours*	*Low*

Large-scale failure of transportation control facility	*Typical example would be failure of air traffic control system (ATS) – caused by software failure or flood, fire, earthquake, bomb etc at specific location. Prolonged industrial action by staff*	*Important ATSs operate on a continental basis and exchange information with other ATSs. Resort to manual measures would lead to cancelling up to 75% of regular flights. Passengers would be stranded and goods not be delivered*	*Software failures could be rectified in hours by loading last known good version. In some regions ATS facilities could be passed to other centres but this would be more difficult for major European and US centres*	*Business thrives on travel though more use could be made of teleconferencing. Tourism could sustain irrecoverable losses as the business is time-sensitive and customers might opt for more local vacations. Losses would also be incurred by those dealing in perishable and other time-sensitive goods*	*If a major ATS centre is physically damaged and there is no viable back-up, flight cancellations and delays could continue for months*	*Short-term*
Large-scale failure of financial services infrastructure – physical	*To qualify under this heading we need to contemplate the inter-bank and inter-institution settlement systems. Physical failure could involve fire, flood, earthquake or bomb. All the big systems have remote back-up sites.*	*The major providers all claim to have survived events such as 9/11. There might be some short-term inconvenience to banks and turbulence in financial markets.*	*Major providers seem to suggest recovery could take place within hours, not days. Position would be different if back-up facilities were hit at the same time as main facilities.*	*In the circumstances, unlikely. However if recovery was not rapid, international investors might start to take protective positions which might then cascade in ways similar to the 2008-2010 banking crisis.*		*Short-term*

Large-scale DDoS – banking	*Short-term DDoS on the Internet facilities of a single bank. The attack would not affect the bank's internal operations or its relationship with other financial institutions as the networks that serve those are not Internet-based.*	*Internet customers of the affected bank would be unable to withdraw, pay in, or check their balance. They would probably try to use the telephone or call at a local branch – both of which would be overloaded.*	*DDoS events tend not to last more than 24 hours because within that time the specific DDoS signature can be determined and then blocked at a technical level. In addition, the longer a DDoS attack is maintained, the greater the chance that the controlling perpetrator is detected.*	*Some businesses and private customers will be inconvenienced and not be able to meet immediate cash needs. There may be some modest knock-on effects for those expecting to be paid. There will also be some additional administrative burden during recovery. Position would be different if a bank's long-term viability were called into question.*		*No*
Large-scale DDoS – health care	*Whilst a DDoS on a single facility is easy to implement, there don't appear to be any obvious targets which cover the critical health requirements of large numbers of people. This might change if greater use was made of centralised health records which are only accessible by hospitals and others over the public Internet*	*Doctors would lack access to medical records and would have to spend longer time analysing the risk factors in treating patients.*	*DDoS events tend not to last more than 24 hours because within that time the specific DDoS signature can be determined and then blocked at a technical level. In addition, the longer a DDoS attack is maintained, the greater the chance that the controlling perpetrator is detected.*	*In the circumstances, unlikely*		*No*

Large-scale DDoS – tax collection / benefits distribution	*As governments increasingly require citizens to interact with services over the Internet, DDoS attacks on the portals are a point of weakness particularly if at the same time local offices are closed and staff reduced*	*In the short-term government loses the ability to collect tax and to pay benefits. Some beneficiaries may be without money or entitlement.*	*DDoS events tend not to last more than 24 hours because within that time the specific DDoS signature can be determined and then blocked at a technical level. In addition, the longer a DDoS attack is maintained, the greater the chance that the controlling perpetrator is detected. Recovery will also depend on the existence of more conventional telephone and local office-based staff.*	*Government will have lost some authority and will have significant explaining to do, including the provision of various remedies to those who have lost out.*		*No*

Large-scale DDoS – essential utilities – hardware & software	*There are well-publicised potential weaknesses in Internet-connected SCADA devices. However to cause a major disruption as opposed to minor upset many such devices would need to be targeted simultaneously- and that would require research about the precise SCADA devices, their IP addresses and their role in the overall grid. Most scenarios envisage denying the SCADA elements the ability to send and receive information/commands to a central facility. There have been illustrations of SCADA commands being able physically to destroy SCADA devices.*	*Partial failure of grids controlling power, water, fuel supply.*	*DDoS events tend not to last more than 24 hours because within that time the specific DDoS signature can be determined and then blocked at a technical level. In addition, the longer a DDoS attack is maintained, the greater the chance that the controlling perpetrator is detected. In July 2010 it was discovered that Siemens SCADA devices could be abused via a hardwired default password, a problem which could not be immediately resolved.*	*While the essential services are unavailable, few businesses will be able to operate and individual life-styles would be very restricted.*	*Short-term remedies such as resort to manual systems and rationing might permit provision of limited services which do not require minute-by-minute SCADA control. The more the attacked system depends on SCADA, the longer the recovery time. However if there are persistent fundamental flaws in devices, further attacks could exploit them later until the flaws are remedied*	*Low*

Zero-day malware (excluding zero-day fundamental flaw in operating system)	*For unprotected PCs that are not backed up, potential loss of functionality plus loss of data. There are hundreds of thousands of malicious applications, though many are variants of a much smaller number of archetypes*	*Solutions are usually found within 24-48 hours but require possession of a viable PC and Internet connection. If data has been backed-up regularly and safely, only 24 hours of activity may have been lost*	*Much malware is self-propagating. The extent of propagation will depend on the speed with which a signature and remedy are found; and the extent to which users update their anti-malware protections. The Melissa virus of 1999 is an example of what can go wrong.*	*As this class of malware is indiscriminate in its victims one can not calculate what propagation effects may take place*	*Over a period vendors of software find solutions. In terms of data corruption, almost complete recovery is possible provided that there has been back-up and a plan for recovery*	*Low*
CII targeted malware	*Malware aimed at specific targets requires significant research for successful execution. The malware must be crafted to fool common anti-malware products. Expert knowledge is needed about the specific systems being targeted; there must be means of introducing the malware.*	*Unlikely to have major immediate impact unless zero-day malware. However a partially successful attack would cause public alarm which would need to be addressed*	*Important facilities may be offline for a few hours or days. Provided there is a contingency plan, recovery would consist of reloading an earlier, known-to-be-reliable version of software and data. Steps may need to be taken to limit the opportunities for re-infection, so that some form of initial diagnosis of the malware would be required*	*Propagation would depend on the extent to which compromised information systems were providing time-critical information and how that information was being used by others. Effects could be limited if there is firm action from government to maintain confidence.*	*Over a period vendors of software find solutions. In terms of data corruption, almost complete recovery is possible provided that there has been back-up and a plan for recovery*	*Low*

Large-scale loss/ compromise of data – banking	*Loss of unencrypted data media or large-scale hack – both are easy to achieve if security is poor. But effects will be limited to individual bank*	*Financial loss to bank and customers. Banking credentials may need to be re-issued – at significant cost*	*Bank may go out of business; individual customers could lose large sums of money. Recovery may require state intervention*	*Individual customers could lose large sums of money. However those seeking to exploit the data will have to limit their activities in order to avoid detection*	*Bank may go out of business; individual customers could lose large sums of money. Recovery may require state intervention*	*Low*
Large-scale loss/ compromise of data – health care	*Loss of unencrypted data media or large-scale hack – both are easy to achieve if security is poor. But effects will be limited to one health authority or one nation*	*Embarrassment for authorities; re-assurance for compromised individuals.*	*Data loss cannot be fully recovered from*	*A few people might die because important medical data is not available when treatment ios being prescribed*	*Data loss cannot be fully recovered from*	*None*
Large-scale loss/ compromise of data — tax collection / benefits distribution	*Loss of unencrypted data media or large-scale hack – both are easy to achieve if security is poor*	*Loss of government income; distress to beneficiaries; loss of confidence in government. Credentials will have to be re-issued*	*Issue of credentials will cost significant amounts and take some time*	*Government could fall through no confidence vote, street demonstrations etc*		*Low*
Successful large scale industrial espionage	*The cyber-environment provides many means for industrial espionage, varying from walking out of a building with unauthorised copies of data on media, through the use of keystroke monitors, Trojans and external hacking.*	*Impact depends not on the method of acquisition but the uniqueness and value of the data acquired – and how it can be exploited.*	*Depends on uniqueness and value of the data acquired. A worst-case scenario might include innovative military technology or where successful exploitation will create wealth and employment*	*Depends on uniqueness and value of the data acquired. In the case of military technology, a nation may find itself a prolonged disadvantage. In the case of civilian technology, workers might lose their job.*	*Depends on uniqueness and value of the data acquired – in a few circumstances there may be no full recovery*	*Depends on uniqueness and value of the data acquired*

EMP (Electro magnetic Pulse)	*EMPs destroy computer hardware. The best known / most extensive example occurs in an air-blast thermonuclear explosion. Experiments have also been carried out using so-called High Energy Radio Frequency guns. The problems are: how to store energy prior to firing, how to release it without destroying the gun, how to direct the energy so that it destroys intended targets rather than "friendly" computers.*	*If the EMP is part of a nuclear explosion then the electronic aspects will be minor compared with the radiation effects, though loss of computer and communications power will exacerbate the circumstances. If we postulate a HERF gun, then the range appears to be in the order of 100s of meters and only computers in range would be affected*	*Assuming the modest range HERF gun, computer hardware would need to be replaced. If back-up data was stored offsite and computer hardware is standard as opposed to specialist, recovery would be possible within 2-3 days*	*For a HERF gun, propagation would be very limited. There is the possibility of collateral damage to adjacent electronic equipment which was intended as the target, If the EMP is associated with a nuclear explosion the main would be radiation and fall-out.*	*If the EMP is associated with a nuclear explosion the main effect would be radiation and fall-out. Computers and data could be restored (at another site) within a few days*	*Only as part of a nuclear explosion .*

Cyberwar attack	*Multi-pronged series of cyber-attacks on a nation state. This would require significant amounts of highly specific research into the targets and also the development of a series of new cyberattack tools – older ones being more likely to fail because they were detected.*	*If the necessary research and tools development has taken place and if the attacks are carefully timed and staged, many critical Internet-based services including e-banking, e-government etc would fail. There would also be temporary extensive loss of all forms of Internet activity*	*A prolonged attack requires a series of specific cyberweapons, used successively. Otherwise recovery of some services likely within a few days provided there are contingency plans in place.*	*Difficult to calculate because of the large number of variables and the variety of sectoral activities potentially affected. Another factor is the resilience of the country being attacked – and that will depend on the existence of alternate routes for providing public services and the quality of any contingency plans, There is a danger for attackers that the greater the impact of their exploit the larger the chance that the results will cascade to effect them as well. A further cause for propagation could be attempted counter-attack or retaliation by victims.*	*Unknown*	*Medium*

Appendix 2

Effects of cyber-related failure coinciding with different large-scale disruption; again these are indicative examples, not actual forecasts:

Event	Immediate Impact	Likely Duration / Recovery factors - immediate	Propagation	Recovery factors – Longer Term (if applicable)	Global Impact?
Pandemic					
Large-scale failure at telecommunications service provider	*Management of a pandemic depends on accurate information about its spread, the ability to provide information and drugs where they are needed. Employers need to know which of their staff are available for work. Families and friends need to keep in touch*	*Recovery likely to be via reverting to previous known good software; then gradual fix of failed software - a few hours? But illness of key staff may cause further delays*	*The problem with pandemics is when a trigger point is reached and there are too few unaffected staff available to keep essential services running. Some patients may die*	*Assuming the failure is software-related and most of the hardware infrastructure is unaffected, recovery would consist of reloading the last previous "known safe" version. This could occur within 24-48 hours*	*To the extent that health authorities world-wide need to be able to track the path of a pandemic and perhaps support each other over the supply of drugs*
Large-scale failure of electricity supply	*Hospitals, doctors surgeries require power. People ill at home require more power than when they are well*	*Electricity is usually supplied via a grid so that some service can be restored in hours. More remote locations may have to wait days, but not much longer. But illness of key staff may cause further delays*	*The problem with pandemics is when a trigger point is reached and there are too few unaffected staff available to keep essential services running. Some patients may die*	*Up to now, most such outages have not lasted more than 24-48 hours*	*To the extent that health authorities world-wide need to be able to track the path of a pandemic and perhaps support each other over the supply of drugs*

Large-scale failure of critical network facility: cable, landing, satellite link or switch	*Management of a pandemic depends on accurate information about its spread, the ability to provide information and drugs where they are needed. Employers need to know which of their staff are available for work. Families and friends need to keep in touch*	*This type of failure may involve loss of some national and international links while keeping local services active. Could be several days or even weeks, depending on severity. ISPs may need to consider limiting bandwidth-hogging applications like video streaming. Telephone companies may need to favour priority customers*	*The problem with pandemics is when a trigger point is reached and there are too few unaffected staff available to keep essential services running. Some patients may die*	*Repair of hardware may take 2 or more weeks, depending on circumstances; but priority emergency communications via re-routing should be possible with 24 hours, provided there is some form of contingency plan*	*To the extent that health authorities world-wide need to be able to track the path of a pandemic and perhaps support each other over the supply of drugs*
Large-scale DDoS – health care	*Management of a pandemic depends on accurate information about its spread, the ability to provide information and drugs where they are needed. Employers need to know which of their staff are available for work.*	*DDoS events tend not to last more than 24 hours because within that time the specific DDoS signature can be determined and then blocked at a technical level. In addition, the longer a DDoS attack is maintained, the greater the chance that the controlling perpetrator is detected. But illness of key staff may cause further delays*	*The problem with pandemics is when a trigger point is reached and there are too few unaffected staff available to keep essential services running Some patients may die*		*To the extent that health authorities world-wide need to be able to track the path of a pandemic and perhaps support each other over the supply of drugs*

Large-scale DDoS – tax collection / benefits distribution	*During a pandemic there is likely to be a greater demand on government-proved benefits*	*DDoS events tend not to last more than 24 hours because within that time the specific DDoS signature can be determined and then blocked at a technical level. In addition, the longer a DDoS attack is maintained, the greater the chance that the controlling perpetrator is detected. But illness of key staff may cause further delays*	*The problem with pandemics is when a trigger point is reached and there are too few unaffected staff available to keep essential services running. Government would probably not suffer in terms of tax collection; but vulnerable users of benefits might run out of funds – and that might cause a political disturbance*		*None*
Large-scale DDoS – essential utilities – hardware & software	*A DDoS SCADA-related failure could impact on facilities needed by hospitals, doctors, etc as well as making the home environment for patients more difficult*	*DDoS events tend not to last more than 24 hours because within that time the specific DDoS signature can be determined and then blocked at a technical level. In addition, the longer a DDoS attack is maintained, the greater the chance that the controlling perpetrator is detected. But illness of key staff may cause further delays*	*The problem with pandemics is when a trigger point is reached and there are too few unaffected staff available to keep essential services running. Some patients will die*		*None*

Zero-day malware	*Although malware is usually not specifically targeted one must assume that some critical health facilities will be affected so that doctors, nurses, patients, etc cannot access important time-critical information or communicate. As a result some patients may die*	*Solutions are usually found within 24-48 hours but require possession of a viable PC and Internet connection. If data has been backed-up regularly and safely, only 24 hours of activity may have been lost. But illness of key staff may cause further delays*	*The problem with pandemics is when a trigger point is reached and there are too few unaffected staff available to keep essential services running*	*Over a period vendors of software find solutions. In terms of data corruption, almost complete recovery is possible provided that there has been back-up and a plan for recovery*	
Large-scale loss/ compromise of data – health care	*Much will depend on what was lost or compromised and the speed with which accurate back-up data can be provided. But successful treatment of patients depends on knowledge of their previous medical history.*	*Much will depend on what as lost or compromised and the speed with which accurate back-up data can be provided*	*Patients may die through non-availability of health history information. If confidential information is lost, public confidence will be affected*	*For lost data: recovery will be swift if back-up exists. For compromised confidential data, recovery in terms of public confidence might never fully occur*	

Very large-scale fire, flood, chemical escape, earthquake					
Large-scale failure at telecommunications service provider (either part of, or separate from triggering event)	*Speedy and effective response depends on accurate reporting of the extent of damage – and the efficient deployment of emergency services. If telephone, cellphone and Internet facilities are knocked out, the only other communications medium would be point-point mobile radio, with a much reduced capability.*	*Recovery time is difficult to predict as the two events will affect each other. Limited cellphone services could be brought in via mobile base-stations within a few days but their capacity would be very limited. Data traffic could use mobile satellite uplinks but here also capacity would be very limited*	*Depends on severity of initial triggering event*	*Difficult to forecast*	*Low*
Large-scale failure of electricity supply provider (either part of, or separate from triggering event)	*Electric power is essential for communications and the emergency services. Those who have lost their homes will need facilities for heating, cooking etc. See also above for implications of loss of communications services*	*Recovery time is difficult to predict as the two events will affect each other. Limited power could be provided by generators, but these in turn need fuel.*	*Depends on severity of initial triggering event*	*Difficult to forecast*	*Low*

Large-scale failure of critical network facility: cable, landing, satellite link or switch provider (either part of, or separate from triggering event)	*There will be local but not necessarily national or international impacts. Telephone and internet are essential for the monitoring of damage, extent of repair, deployment of workmen etc*	*Recovery time is difficult to predict as the two events will affect each other. These networks have a route-around facility and it may be possible to install temporary equipment to give limited service to some high priority customers*	*Depends on severity of initial triggering event*	*Difficult to forecast*	*Low*
Large-scale DDoS – banking	*In the very short-term money and cash will be unimportant. A banking DDoS during the recovery period would increase anxiety among the population*	*DDoS events tend not to last more than 24 hours; but recovery might be delayed and customers could panic*	*The main propagation feature would be panic*		*Low*

Large-scale DDoS – health care	*These events will cause many casualties who will require treatment. Health professionals will want access to patient records and other data*	*DDoS events tend not to last more than 24 hours; but recovery might be delayed and customers could panic*	*If it has been possible to implement a proper contingency plan for health records propagation effects will limited to the most immediate and seriously affected victims. In a very large-scale incident it is possible that facilities and their back-ups are lost. But for less seriously affected patients doctors would be able to ask them about their medical histories,*		*Low*

Large-scale DDoS – tax collection / benefits distribution	*In the very short term no one will care about tax collection or benefits distribution.*	*In the medium term governments will be expected to provide all manner of emergency support and benefits – and will want to know the identity and history of those requesting them. But DDoS events tend not to last more than 24 hours*	*If it has been possible to implement a proper contingency plan for the tax collection/ benefits systems, propagation effects will limited to the most immediate victims as they may have lost their own records. However in a very large-scale incident it is possible that central government facilities and their back-ups are lost.*		*Low*
Zero-day malware	*Although malwars is usually not specifically targeted, many computers will be affected and to will be unavailable to assist the broader recovery*	*Getting the fixes from vendors on to the affected PCs may take longer because of the overall disaster conditions*	*Will depend on extent of triggering disaster*		

Large-scale loss/ compromise of data – health care	*Much will depend on what was lost or compromised and the speed with which accurate back-up data can be provided. But successful treatment of patients is improved by knowledge of their previous medical history.*	*Much will depend on what as lost or compromised and the speed with which accurate back-up data can be provided*	*Possible secondary medical effects because of lack of immediate treatment, including patient death*	*Much will depend on what as lost or compromised and the speed with which accurate back-up data can be provided*	*Low*
Large-scale loss/ compromise of data – banking	*In the very short term there will be no need for cash*	*Much will depend on what as lost or compromised and the speed with which accurate back-up data can be provided*	*If there is no quick fix, people and businesses will lack cash – and will panic*	*Much will depend on what as lost or compromised and the speed with which accurate back-up data can be provided*	*Low*
Large-scale loss/ compromise of data — tax collection / benefits distribution	*In the very short term - none*	*In the longer term victims will expect remedial action and compensation from the government – which would lose authority if unable to respond*	*If government remains incapacitated law and order will break down*	*Recovery will depend on the availability of back-up data and computers*	*Low*

Banking-related Crisis					
Large-scale failure at telecommunications service provider Large-scale failure of electricity supply Large-scale failure of critical network facility: cable, landing, satellite link or switch Large-scale DDoS – banking Large-scale DDoS – essential utilities – hardware & software Software failure – large-scale system – generic Large-scale loss/ compromise of data – banking (separate from banking crisis)	*In a banking crisis there is already an atmosphere of panic as customer worry about their deposits and savings, businesses are concerned about financing cash flows, and governments about economic stability. The inability to communicate with a bank would exacerbate the crisis*	*Much will depend on the nature of the crisis and any underlying factors. In the events of 2008-2010 an initial small problem – failures of loans associated with sub-prime mortgages, cascaded globally. There may be no immediate recovery*	*Much will depend on the nature of the crisis and any underlying factors.*	*Much will depend on the nature of the crisis and any underlying factors.*	*Could be high*
Zero-day malware	*Although malware is usually not specifically targeted, many computers will be affected with the result that owners will not be able to communicate with banks*	*Much will depend on the nature of the crisis and any underlying factors. In the events of 2008-2010 an initial small problem – failures of loans associated with sub-prime mortgages, cascaded globally. There may be no immediate recovery*	*Much will depend on the nature of the crisis and any underlying factors.*	*Much will depend on the nature of the crisis and any underlying factors.*	*Could be high*

References

ACLU (American Civil Liberties Union) (2010), *Tell Google Not to Enter Into an Agreement With the NSA*, Blog of Rights, 5 February.

Anderson, Boehme, Clayton, Moore. (2008). *Security Economics and the Internal Market.* Available: http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec. Last accessed 17 December 2010.

Anderson, J.Q. and L. Rainie (2010), *The Future of the Internet*, Pew Research Center, Washington, D.C.

APEC (Asia Pacific Economic Cooperation) (2002), *APEC Leaders' Statement On Fighting Terrorism And Promoting Growth*, Los Cabos, Mexico.

Assange, J. (2006). *The Curious Origins of Political Hacktivism.* Available: http://www.counterpunch.org/assange11252006.html. Last accessed 18 December 2010.

Coaffe, J. (2003), *Terrorism, Risk and the City: The Making of a Contemporary Urban Landscape*, Ashgate, London.

Backhouse, J. and G. Dhillon (2000), *Information system security management in the new millennium*, Communications of the ACM, Vol. 43, No. 7, pp. 125-128.

Ballard, M. (2010), *UN rejects international cybercrime treaty*, Computer Weekly, 20 April.

BBC News (2007), *Rush on Northern Rock continues*, 15 September, BBC, London.

BBC News (2010), *Floodwater cleared at BT exchange*, 1 April, BBC, London.

Berinato, S. (2006). *Attack of the Bots*, Wired Magazine, Vol. 14, No. 11.

Bond,A. (2010). *Siemens Stuxnet attack sophisticated, targeted.* Available: http://www.controlglobal.com/industrynews/2010/163.html. Last accessed 13 August 2010.

Borg, S. (2005), *Economically Complex Cyberattacks*, IEEE Security and Privacy, Vol. 3, No. 6, pp. 64-67.

Brandt, A. (2005), *Alleged Botnet Crimes Trigger Arrests on Two Continents*, PC World, 5 November.

Brown, I., L. Edwards and C. Marsden (2009), *Information security and cybercrime*, in L. Edwards and C. Waelde (eds.), *Law and the Internet, 3rd edition*, Hart, Oxford, pp. 671-692.

Bruijne, M. de and M.J.G. van Eeten (2007), *Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment*, Journal of Contingencies and Crisis Management, Vol. 15, No. 1, pp. 18-29.

Bugtraq (2001), *Levin/Citibank*, http://bugtraq.ru/library/books/attack3/intro/#levin

Burgess, C. (2008). *Nation States' Espionage and Counterespionage.* Available: http://www.csoonline.com/article/337713/nation-states-espionage-and-counterespionage. Last accessed 30th September 2010.

Cameron, E. (2007), House of Lords Debate c.424, 13 November, London.

Carlberg, K., R. Desourdis, J. Polk and I. Brown (2003), *Preferential emergency communications: from telecommunications to the Internet*, Springer, Massachusetts.

Cashell & others. (2004). The Economic Impact of Cyber-Attacks. *CRS Report for Congress*..

Centre for the Protection of National Infrastructure (2010), *What we do*, www.cpni.gov.uk/About/whatWeDo.aspx

Center for Strategic and International Studies (2008), *Securing Cyberspace for the 44th Presidency*, Center for Strategic and International Studies, Washington, D.C.

Clark, W.K. and P.L. Levin (2009), *Securing the Information Highway: How to Enhance the United States' Electronic Defenses*, Foreign Affairs, Nov/Dec.

Clarke, R A and Knake, R K (2010). *CyberWar, the next threat to national security and what to do about it*. New York: Ecco/HarperCollins. 290 pp.

Commission of the European Communities (2008), *Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems*, COM/2008/0448 final, European Commission, Brussels.

Commission of the European Communities (2009), *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, COM(2009) 149 final, European Commission, Brussels.

Cornwall, H. (1985), *Hacker's Handbook*, Century, London.

Cornwall, H. (1987), *DataTheft*, Heinemann, London.

Council of Europe (2008), *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime*, Council of Europe, Strasbourg.

Council of the European Union (2005), *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems*, OJ L 69, 16.3.2005, p. 67.

Council of the European Union (2008), *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, OJ L 345, 23.12.2008, p. 75.

Crabbyolbastard. (2010). *EMP | Electrical Grids | A Thought Experiment.* Available: http://crabbyolbastard.wordpress.com/2010/10/25/emp-electrical-grids-a-thought-experiment/. Last accessed 18 December 2010.

Cryptome (2006), *Michael John Smith*, http://cryptome.org/michael-smith.htm. Last accessed 24 April 2010.

DEFRA (Department for Farming and Rural Affairs) (2006), *Groceries Report 2006*, https://statistics.defra.gov.uk/esg/reports/Groceries%20paper%20May%202006.pdf

Denham, J. (2009), *Lecture to the Royal Society for the encouragement of Arts, Manufactures & Commerce by the Secretary of State for Communities and Local Government*, www.communities.gov.uk/speeches/corporate/rsaevent2009

Dutton, W.H., E.J. Helsper and M.M. Gerber (2009), *The Internet in Britain: 2009*, University of Oxford, Oxford.

Dyer, C. (2010). *HC498: Submission to UK House of Commons Select Committee: Scientific Advice in Emergencies: Solar Flares.* Available: http://www.publications.parliament.uk/pa/cm201011/cmselect/cmsctech/writev/498/m05.htm. Last accessed 17 December 2010.

The Economist (2010), *Ne'er the twain*, 22 April.

Eeten, M.J.G. van and J.M. Bauer (2008) *Economics of Malware: Security Decisions, Incentives and Externalities*, DSTI/DOC(2008)1, OECD, Paris.

Ernesto. (2010). *Behind The Scenes at Anonymous' Operation Payback.* Available: http://torrentfreak.com/behind-the-scenes-at-anonymous-operation-payback-111015/. Last accessed 18 December 2010.

European Commission (2009), *Report on Cross-border e-Commerce in the EU*, SEC(2009) 283 final, European Commission, Brussels, p. 5.

ENISA (European Network and Information Security Agency) (2009), *Cloud Computing: Benefits, risks and recommendations for information security*, ENISA, Crete.

ENISA. (2010). *Report on Secure routing technologies.* Available: www.enisa.europa.eu/act/res/technologies/tech/routing/.../fullReport. Last accessed 18 December 2010.

Eurostat (2008), *Data in Focus* 48/2008, European Commission, Luxembourg.

Evans, L. (2001), *Mafiaboy's Story Points to Net Weaknesses*, PC World, 24 January.

F-Secure (2006), *F-Secure Virus Descriptions: Melissa*, www.f-secure.com/v-descs/melissa.shtml. Last accessed 24 April 2010.

Falliere, N. (2010). *Exploring Stuxnet's PLC Infection Process.* Available: http://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process. Last accessed 28 September 2010.

Finkelstein, A. (2000), *Y2K: a retrospective view*, Computing & Control Engineering Journal, Vol. 11, No. 4, pp. 156-157.

G8 Justice and Interior Ministers (2003), *G8 Principles for Protecting Critical Information Infrastructures*, www.justice.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf

GAO (Government Accountability Office) (1996), *GAO Report AIMD 96-84*, www.gao.gov/archive/1996/ai96084.pdf

GAO (2009), *Influenza Pandemic*, www.gao.gov/new.items/d108.pdf

GAO (2010), *Cyberspace, United States faces Challenges in Addressing Global Cybsecurity and Governance*, GAO-10-606 http://www.gao.gov/products/GAO-10-606

Gorman, S. (2009), *Electricity Grid Penetrated by Spies*, The Wall Street Journal, April 9, p. A1.

Gartner. (2009), *Gartner Says Internet Bandwidth Supply May Not Meet Demand During a Pandemic*, http://www.gartner.com/it/page.jsp?id=1217613

Graham, F. (2009). *Gaza crisis spills onto the web* . Available: http://news.bbc.co.uk/1/hi/technology/7827293.stm. Last accessed 18 December 2010.

Halliday and Arthur. (2010). *WikiLeaks: Who are the hackers behind Operation Payback?.* Available: http://www.guardian.co.uk/media/2010/dec/08/anonymous-4chan-wikileaks-mastercard-paypal?intcmp=239. Last accessed 18 December 2010.

Hamilton Consultants (2009), *Economic Value of the Advertising-Supported Internet Ecosystem*, Interactive Advertising Bureau, Washington, D.C.

Herley, C. and D. Florencio (2008), *A Profitless Endeavor: Phishing as Tragedy of the Commons*, New Security Paradigms Workshop, Lake Tahoe, California.

Hesseldahl, A. (2009), *White House appoints Cybersecurity Czar*, Businessweek, 22 December.

Hines, Cotilla-Sanchez, Blumsack. (2010). *Do topological models provide good information about electricity infrastructure vulnerability?.* Available: http://chaos.aip.org/resource/1/chaoeh/v20/i3/p033122_s1?isAuthorized=no. Last accessed 17 December 2010.

Home Security Newswire (2009), *Hamas, Hezbollah employ Russian hackers for cyber attacks on Israel*, Homeland Security News, 15 June.

HM Treasury (2009a) *Putting the Frontline First: Smarter Government*, Cm. 7753, The Stationary Office, London, pp. 22—25.

HM Treasury (2009b), *Operational Efficiency Programme.* Available: http://www.hm-treasury.gov.uk/vfm_operational_efficiency.htm. Last accessed 4 May 2010.

House of Lords European Union Committee (2010), *Protecting Europe against large-scale cyber-attacks*, HL Paper 68, The Stationary Office, London.

Hunker, Hutchinson, Margulies. (2008). *Role and Challenges for Sufficient Cyber-Attack Attribution.* Available: http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf. Last accessed 18 December 2010.

Information Warfare Monitor (2009) *Tracking GhostNet*, www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

Information Warfare Monitor (2010), *Shadows in the Cloud*, www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0

ICANN (Internet Corporation for Assigned Names and Numbers) (2007), *Root server attack on 6 February 2007*, ICANN, Marina del Rey.

Interpol (2009) *IT Crime – Regional working parties*, www.interpol.int/Public/TechnologyCrime/WorkingParties/

ITU (International Telecommunication Union) (2007) *Cybersecurity Guide for Developing Countries*, ITU, Geneva.

ITU (2009a), *ITU Toolkit for Cybercrime Legislation*, ITU, Geneva.

ITU (2009b), *Understanding Cybercrime: A Guide for Developing Countries*, ITU, Geneva.

ITU (2009c), *National Cybersecurity/CIIP Self-Assessment Tool*, ITU, Geneva.

ITU (2010), *Measuring the Information Society 2010*, ITU, Geneva.

Keizer, G. (2009), *Almost all Windows users vulnerable to Flash zero-day attacks*, Computer World, 27 July.

Kent, S. (2006). *Securing the Border Gateway Protocol (S-BGP*. Available: https://www.arin.net/participate/meetings/reports/ARIN_IX/PDF/S-BGP.pdf. Last accessed 18 December 2010.

Kshetri, N. (2006). The simple economics of cybercrimes. *Security and Privacy, IEEE*. 4 (1), 33-39.

Kutrtz, G. (2010), *Operation "Aurora" Hit Google, Others,* McAfee Security Insights Blog, 14 January.

Layne, K & Lee, J. (2001). Developing fully functional E-government: A four stage mod. *Government Information Quarterly*. 18 (2), 122-136.

Leppard, D. and C. Williams (2009), *Jacqui Smith's secret plan to carry on snooping*, The Sunday Times, 3 May.

Lewis, J.A. (2009), *The "Korean" Cyber Attacks and Their Implications for Cyber Conflict*, Center for Strategic and International Studies, Washington, D.C.

Libicki, M.C. (2009), *Cyberdeterrence and Cyberwar*, RAND Corporation, Santa Monica.

McConnell, M. (2010), *We're losing the cyber-war. Here's the strategy to win it,* Washington Post, 28 February.

McMillan, R. (2010), *Spanish Police Take Down Massive Mariposa Botnet,* PC World, 2 March.

metac0m . (2003). *What Is Hacktivism? 2.0.* Available: http://www.thehacktivist.com/whatishacktivism.pdf. Last accessed 18 December 2010.

Menn, J. (2010), *Fatal System Error,* Public Affairs, New York.

Mukhopadhyaya, K and Sinha, B P. (1992). *Reliability analysis of networks using stochastic model . Information Sciences* . Volume 65, Issue 3, 225-237 .

Motter, A. and L. Ying-Cheng (2002), *Cascade-based attacks on complex networks,* Physical Review, E66, 065102(R).

Mussington, D. (2002), *Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development*, RAND Corporation, Santa Monica.

NATO (North Atlantic Treaty Organisation) (2008), *Defending against cyber attacks*, at www.nato.int/issues/cyber_defence/practice.html

Nakashima, E. (2010), *Google to enlist NSA to help it ward off cyberattacks*, Washington Post, 4 February.

NIST. (2010). *Presentation on Effectively and Securely Using the Cloud Computing Paradigm v26.* Available: http://csrc.nist.gov/groups/SNS/cloud-computing/. Last accessed 19 December 2010.

Noam, E.M. and H. Sato (1995), *Kobe's lesson: Dial 711 for 'open' emergency communications*, Telecommunications Policy, Vol. 19, No. 8, pp. 595-598.

NRC (2010) National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, National Academies Press, Washington

O'Murchu, L. (2010). *An in depth look into Stuxnet.* Available: http://www.virusbtn.com/conference/vb2010/abstracts/LastMinute7.xml. Last accessed 29 September 2010

Oak Ridge National Laboratory. (2010). *Electromagnetic Pulse: Effects on the U.S. Power Grid.* Available: http://survive-emp.com/fileadmin/White-Papers/Solar-Storms/ferc_Executive_Summary_EMP_Impact_on_grid_jan_2010.pdf. Last accessed 18 December 2010.

OECD (Organisation for Economic Cooperation and Development) (2002), *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, Recommendation of the Council adopted 25 July 2002, OECD, Paris.

OECD (2006) *The Development of Policies for the Protection of Critical Information Infrastructures (CII):* DSTI/ICCP/REG(2006)15/FINAL, OECD, Paris

OECD (2007), *Malicious Software (Malware): A Security Threat to the Internet Economy*, Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL, OECD, Paris.

OECD (2008a), *The Future of the Internet Economy: A Statistical Profile*, OECD, Paris.

OECD (2008b), *Recommendation of the Council on the Protection of Critical Information Infrastructures*, C(2008)35, OECD, Paris.

Omand, D (2010). *Securing the State*. London: Hurst & C.

Orrey, K. (2009), *Penetration Testing Framework.* Available: http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html. Last accessed 2 May 2010.

Owen , C. (2010). *HC499: Submission to UK House of Commons Select Committee: Scientific Advice in Emergencies: UCL Institute for Risk and Disaster Solar Flares.* Available: http://www.publications.parliament.uk/pa/cm201011/cmselect/cmsctech/writev/498/m17.htm. Last accessed 17 December 2010.

Perrin, C. (2010). *The danger of complexity: More code, more bugs.* Available: http://blogs.techrepublic.com.com/security/?p=3076. Last accessed 13 August 2010

Peters, K., L. Buzna and D. Helbing (2008), *Modelling of cascading effects and efficient response to disaster spreading in complex networks*, International Journal of Critical In

Pham. H & Galyean W G . (1992). *Reliability analysis of nuclear fail-safe redundancy* . Reliability Engineering & System Safety . Volume 37, Issue 2 , 109-112 .

Quigley, K. (2004), *The Emperor's New Computers: Y2K (Re)visited*, Public Administration, Vol. 82, No. 4, pp. 801-829.

Reding, V. (2008), *Digital Europe: The Internet Mega-Trends That Will Shape Tomorrow's Europe*, European Internet Foundation, Brussels, p. 2.

Rivera, M. (2009), *Could Swine Flu Take the Internet Down?* Wall Street Journal Blogs, 2 October.

Rotenberg, M (2010) Statement before the US House of Representatives Committee on Science and Technology, *Planning for the Future of Cyber Attack Attribution,* July 15, 2010, Washington, DC

Rudolph, J.W. and N.P. Repenning (2002), *Disaster dynamics: Understanding the role of quantity in organizational collapse*, Administrative Science Quarterly, March.

Schwartau, W (1994). *Information Warfare*. New York: Thunder's Mouth Press. 431.

Shachtman, N. (2008), *Georgia Under Online Assault,* Wired Danger Room, 10 August.

Shughart, W.F. (2006), *Katrinanomics: The politics and economics of disaster relief*, Public Choice, Vol. 127, No. 1, pp. 31-53.

Singel, R. (2008), *Fiber Optic Cable Cuts Isolate Millions From Internet, Future Cuts Likely*, Wired Threat Level, 31 January.

Sommer, P. (1998), *Intrusion Detection Systems as Evidence*, First International Workshop on Recent Advances in Intrusion Detection, Louvain-la-Neuve, Belgium.

Sommer, P. (2004). The future for the policing of cybercrime. *Computer Fraud and Security*. 2004 (1), 8-12.

Sommer, P and Hosein, I (2009). *Briefing on the Interception Modernisation Programme*. London : LSE Policy Engagement Network. 1-59. Available from http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf

SpamFighter (2009), *BSNL Cautioned Against Possible Malware in Huawei Equipments,* www.spamfighter.com/News-12437-BSNL-Cautioned-Against-Possible-Malware-in-Huawei-Equipments.htm

Sterling, B. (2010). *Advanced Persistent Threat Attack.* Available: http://www.wired.com/beyond_the_beyond/2010/01/the-advanced-persistent-threat-attack/. Last accessed 29 September 2010.

SWIFT (Society for Worldwide Interbank Financial Telecommunication) (2009). *Swift History*, www.swift.com/about_swift/company_information/swift_history.page

Symantec (2010), *Symantec Global Internet Security Threat Report*, Vol. 15, Symantec, Mountain View, California.

Thomas, M. (2000), *Further Myths of the Year 2000*, Computing & Control Engineering Journal, Vol. 11, No. 4, pp. 158-159.

Thornburgh, N. (2005), The Invasion of the Chinese Cyberspies, Time, Washington, D.C.

Times of India *Cyber war: Indian Army gearing up.* Available: http://timesofindia.indiatimes.com/articleshow/6187297.cms?prtpage=1. Last accessed 12 August 2010.

Towards a Future Internet (2010), *Interim report*, European Commission, Brussels.

UK Office of Cyber Security (2009) *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*, Parliament Command Paper 7642, London.

UK Cabinet Office (2009), *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards,* www.cabinetoffice.gov.uk/media/349103/strategic-framework.pdf

UK Payments Council (2010), *The Way We Pay 2010: The UK's Payment Revolution*, Payments Council, London.

UK Resilience (2009), *Responding to emergencies*, www.cabinetoffice.gov.uk/ukresilience/response/response.aspx

UN (United Nations) (2010a), *Twelfth United Nations Congress on Crime Prevention and Criminal Justice: Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime*, A/CONF.213/9, United Nations, Geneva.

UN (2010b), *Twelfth United Nations Congress on Crime Prevention and Criminal Justice: Report of Committee II on agenda item 8 and Workshop 2*, A/CONF.213/L.4/Add.1, United Nations, Geneva.

UNCTAD (United Nations Conference on Trade and Development) (2009), *Information Economy Report 2009*, UNCTAD, Geneva, p. xii.

United States Air Force. (2010). *CyberSpace Operations: Air Force Doctrine Document 3-12.* Available: http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf. Last accessed 17 December 2010.

U.S.-Canada Power System Outage Task Force (2004), *Natural Resources Canada – Canada - U.S. Power System Outage Task Force Interim Report, 2004.*

US Department of Justice (2004), *G8 Background*, www.justice.gov/criminal/cybercrime/g82004/g8_background.html

US Executive Office of the President (2010), *The Comprehensive National Cybersecurity Initiative*, www.whitehouse.gov/sites/default/files/cybersecurity.pdf

US Secretary of Defense (2009), *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations*, memorandum dated June 23, www.govexec.com/nextgov/0609/gates_cybercommand_memo.pdf

US-China Economic and Security Review Commission (2009), *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman, McLean, Virginia.

Vijayan, J. (2010), *Reported Google-NSA alliance sets off privacy alarms*, Computerworld, 4 February.

Visa Europe (2009), *Annual Report*, Visa Europe, London.

Volk, W. (2010). *Eyjafjallajokull fallout: What did Iceland's volcano's explosion cost travelers?*. Available: http://www.gadling.com/2010/04/27/eyjafjallajokull-icelands-volcanos-explosion-cost/. Last accessed 18 December 2010.

Weiner, Norbert (1962), *The mathematics of self-organising systems*, in: Machol & Gray, *Recent developments in information and decision processes*, Macmillan, New York.

Weiss, G. (1996), *The Farewell Dossier*, Studies in Intelligence, Central Intelligence Agency, Langley.

Winter, P. and J. Wilson (2000), *Britain grinds to a halt as Blair's pleas are ignored*, The Guardian, 24 September.

Wong, K (1983), *Computer Crime Casebook*, BIS Applied Systems, London, pp. 1-48.

Young, T. (2009), *Foiling a thoroughly modern bank heist*, Computing, 19 March.

Zetter, K. (2010), *Microsoft Learned of IE Zero-Day Flaw Last September*, Wired Threat Level, 21 January.

Zhuge, J., T. Holz, X. Han, J. Guo and W. Zou (2007), *Characterizing the IRC-based botnet phenomenon*, Informatik Tech. Report TR-2007-010, http://honeyblog.org/junkyard/reports/botnet-china- TR.pdf