The 'Perfect Storm':

Net Neutrality and Next Generation Network Deployment

Christopher T. Marsden LL.B., LL.M.,
Cambridge/Oxford/Essex Universities
and RAND Europe[1]

[1] Honorary Industrial Policy Fellow, University of Cambridge Computer Laboratory; Visiting Fellow, Centre for Socio-Legal Studies, Oxford University; Teaching Fellow, University of Essex School of Law; Senior Analyst, RAND Europe. Email: ctmarsden@yahoo.co.uk
Comments welcome. This paper and any views therein are personal and should not be interpreted as referring to the view of any of the above-named organisations.
I wish to thank (amongst numerous others) : Dave Clark and Bill Lehr; Mark Handley and Jon Crowcroft; Ian Brown and Lilian Edwards; Jonathan Cave; Neil Robinson; Martin Cave; Eli Noam; Jonathan Aronson; Kenn Cukier; the participants in the 2006 TPRC and 2005/6 Wharton Media Law Symposia. All errors and omissions are mine alone.

CHAPTER 1 Forecasting the 'Perfect Storm'

Policy for broadband deployment is at a critical tipping point (again…). This time its for real. How much Quality of Service (QoS) will there be in Next Generation Networks (NGNs)? That is being decided by regulators publicly now, but has been the subject of private standards setting efforts since at least the beginning of 2000 (when work on standardising the IP Multimedia Subsystem (IMS) was commenced). Regulatory analysts often 'don't get it' because they focus on narrow questions of telecoms regulation. There are at least two other critical factors at play: concern over illegal and inappropriate content (such as child pornography, copyrighted music and latterly video files being inappropriately shared, and malware including spam); and the security agenda which aims to enforce QoS to separate 'good' or preferred from 'bad' or discriminated-against packets. There is a legitimate concern that this represents a division between the rich and powerful senders of packets and the lesser content types. These three concerns, telecoms, content and security, are coming together. Policies made in their relative policy arenas are tending to the same result in terms of incentives to deploy NGNs – to change the Internet forever, to become faster, safer but more closed.

1.1 Approach and Definitions

Note immediately the overlap among technologies, applications that rely on them, competition in networks and applications and the role of the regulator. We emphasise that factors can be considered discretely: therefore, these analyses form a necessary starting point for a more integrative discussion. Foresight exercises in broadband policy have been carried out in various territories, for instance the Netherlands[2] and European Commission[3] exercises of 2002-3, and the OECD report of 2006[4]. Broadband policy is under continual review as part of the i2010 strategy of the European Council[5], and the review of the Communications Regulatory Framework. This policy approach is

[2] Horlings, Botterman, Cave, Ligtvoet, de Vries (2002) Accelerated Broadband Roll-Out for the Netherlands: A Review of Economic Benefits, Directoraat Generaal Telecommunicatie en Post (MR-1654-NDGTP; September. Santa Monica: RAND.

[3] Botterman, Anderson, van Binst, Cave, Libicki, Ligtvoet, te Velde, de Vries (2003) Enabling the Information Society by Stimulating the Creation of a Broadband Environment in Europe: Analyses of Evolution Scenarios for Future Networking Technologies and Networks in Europe, DG Information Society (MR-1579). Santa Monica: RAND.

[4] See Bohlin, E., Forge, S. and Blackman (2006) C. Chapter 2, Telecoms Infrastructure to 2030, pp51-148 in OECD (2006) Infrastructure to 2030: Telecom, Land Transport, Water and Electricity, OECD: Paris.

[5] Van Oranje, Simmons, Kahan, Botterman, Lundin (2005) The Spring Council Review: Implications for Information Society Policy Options, Report for the European Commission, DG Information Society.

moving away from immediate national, and medium-term European, law and policy, to consider a 'next generation' of broadband technologies and their deployment. Given the broad move towards all-Internet Protocol (IP) networks, described commonly as 'Next Generation Networks' (NGNs), this is appropriate[6].

We note that there is no such thing as an inherently 'disruptive technology', but rather technologies that can disrupt markets and social structures[7]. We do not therefore focus on the undoubted potential for extremely high bandwidth to develop, in initiatives that arise outside market, regulatory and social structures, or are not themselves reshaped by structural changes to which they give rise, though the developments in for instance the Internet2 project are well-known[8]. The need for a fresh approach considering economic and social issues as part of technology deployment has been emphasised by the National Science Foundation in the US, with emphasis on Quality of Service and security, the approach we also adopt[9]. We therefore project into a more fully-realised broadband future, rather than specialized research and academic networks. The discussion will focus on possible developments of NGNs[10].

Broadband continues to require definition, as a term of art rather than science. It is defined by reference to its inverse: narrowband[11]. The Dutch government stated:

> 'broadband' is defined in terms of its functionality, not in terms of capacity or technology. Broadband is a continuously available connection suitable for good quality audio-visual applications and the exchange of large data files. With narrowband, one user at a time can use one service only. (Super-)broadband allows multiple users to use different services at the same time, via different platforms.[12]

It may be that in time 'super broadband' will be redefined as normal broadband. In the Netherlands, current broadband speeds are in the 2-20Mbps range, while in Ireland the standard consumer offer is in the 256Kbps to 1Mbps range. In Japan, broadband is offered as standard at

---

[6] See Cave, M., Prosperetti, L. and Doyle, C. (2006) Where are we going? Technologies, markets and long-range public policy issues in European communications, Information Economics and Policy, 18:3, at 242-255.

[7] See Robinson, Neil, David Ortiz, Andreas Ligtvoet, Maarten Botterman, Lorenzo Valeri, Rebecca Shoob, Eddy Nason (2006) Security Challenges to the Use and Deployment of Disruptive Technologies, TR-406-EC, Santa Monica: RAND. See further Christensen, Clayton M. (1997). The Innovator's Dilemma. Harvard Business School Press.. Also see Bower, J., & Christensen, C. (1995). Disruptive technologies: Catching the wave. Harvard Business Review, January-February, 43-53. An important element to the disruptive nature of such technologies is their market impact: see Schumpeter, J. (1975) Capitalism, Socialism and Democracy New York: Harper, [orig. pub. 1942], pp. 82-85 on the concept of 'creative destruction'. The original concept can be traced through Schumpeter to Karl Marx.

[8] http://www.internet2.edu/

[9] See Clarke, D. (2005) FIND and Architecture: A new NSF initiative, at http://find.isi.edu/presentation_files/Clark_Arch_Security.pdf

[10] Talbot, D. (2006) Toward a High-Definition YouTube, MIT Technology Review 26 October, at http://www.technologyreview.com/read_article.aspx?id=17654&ch=biztech&sc=&pg=2 He explains that 400gbps is the expected throughput of Internet2 in 2007.

[11] In US, the FCC "generally defines broadband service as data transmission speeds exceeding 200Kbps" (see http://www.fcc.gov/cgb/consumerfacts/highspeedinternet.html) . See CNET BB meter for lists of BW speeds in US (http://reviews.cnet.com/7020-7973_7-0.html?tag=bbw) which show a range of 1.8-3.0 Mbps (downstream) as of October 2006.

[12] Government of the Kingdom of the Netherlands: Ministry of Economic Affairs (2003) The Broadband Paper: A Question of Pace and Better Utilisation, at 5.

100Mbps[13]. There is already a very wide range of broadband on offer, but it shares the characteristic of being 'always-on', and of sufficient speed to permit high quality files (such as video) to be transferred. The interoperability and sector/service convergence of the broadband world should drive a convergence of speeds. This is an important issue: whether the world will separate into different-speed 'lanes' with crash barriers defined by different applications and ways of accessing data, or will converge on a common infrastructure/service offer, with application differences driven by and responsive to demand changes.

In particular we identify four distinctions among broadband technologies. These are: Symmetry versus Asymmetry; Urban versus Rural; Wired versus Wireless; New or upgraded plant versus twisted pair copper (or in the US coaxial) Plain Old Telephone Service (POTS). The four issues interrelate, but offer distinctive technological paths into the future and demonstrate the range of deployment possibilities for broadband. We offer initial thoughts in the following four paragraphs.

Symmetry is of particular interest for enterprise solutions. Many smaller enterprises, particularly of the Small Office/Home Office (SOHO) type, currently rely on domestic broadband connections, which are configured for downloading rather than uploading. The asymmetry of such connections is often a 10:1 ratio or higher (maximum download speed is 1Mbps but upload speed is 200Kbps or even 100Kbps). This provides a quality-based 'entry barrier' – which is one reason why it persists, and why the price differentials depart from cost-justified tariffs even accounting for congestion. Contention[14] and 'traffic shaping' affect quality. These ratios reflect the perception that home users are generally passive viewers of content developed by professionals. Peer-to-peer networks and other user-generated content and application developments are eroding this distinction but it has remained a constant in the first five years of broadband[15]. In the case of the SOHO enterprise, hosting of an electronic (e-) commerce website or online marketing activities may lead to the need to upgrade to more symmetrical service[16]. Currently the price difference between business and consumer broadband products is very high[17]. Figure 1 offers a simplified view of consumer supply-demand curves, illustrating where broadband supply outstrips demand and vice versa in a series of technological advances.

---

[13] Latest OECD numbers

[14] 20:1 for businesses, 50:1 for home, but delivered speeds that reflect/punish increasing uptake

[15] See Karagiannis, Thomas, Pablo Rodriguez, Dina Papagiannaki (2005) Should Internet Service Providers Fear Peer-Assisted Content Distribution? Internet Measurement Conference (IMC), Berkeley, CA, USA.

[16] With productivity implications: see Brynjolfsson, Erik and Hitt, Lorin M., 'Computing Productivity: Firm-Level Evidence' (June 2003). MIT Sloan Working Paper No. 4210-01. http://ssrn.com/abstract=290325 and Erik Brynjolfsson, 'The IT Productivity Gap' (July 2003). Optimize, Issue 21.

[17] For instance the UK incumbent British Telecom has ceased to offer its Symmetrical DSL (SDSL) product at 2Mbps, with forecast demand having failed to materialise as businesses choose Asymmetric DSL (ADSL) products

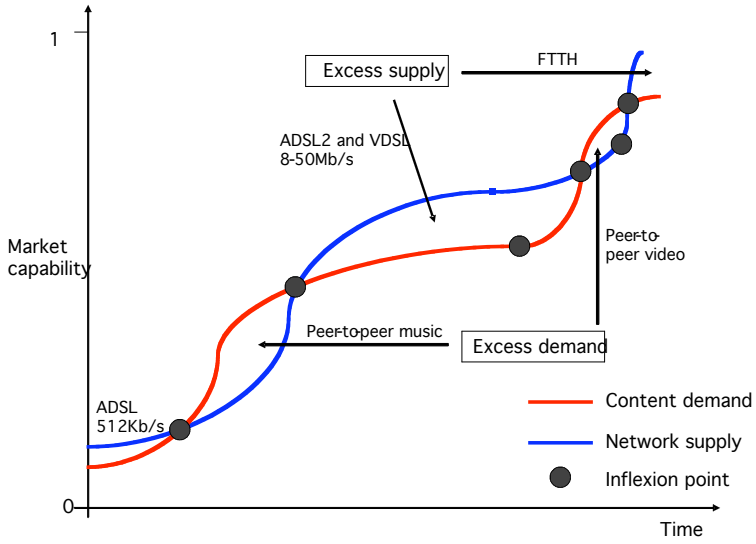


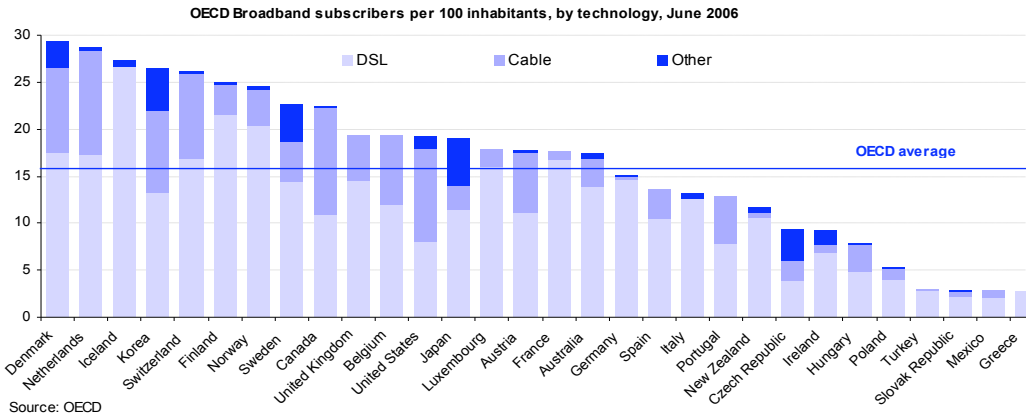
Figure 1: Possible Development of the Supply–Demand Curves for Broadband

The figure could be dated according to the development of an urban/rural, sophisticated/basic broadband market.

In the NGN future, where products will be offered at 100Mbps and more in the near future, the issue of symmetrical small business connections will continue to be an important issue. Technologies and charging models for traffic shaping and capacity management will also develop. We expect significant disparity in rates and capacity available within the developed and developing world, and between rural and urban locations. High bandwidth services such as enterprise-class high definition video could be provided via IP video or Radio Frequency overlay[18]; their efficiency will depend on the number of channels. How this efficiency relates to broadband bandwidth and provisioning architecture will drive investment and Research and Development (R&D) decisions in fibre-optics and DWDM networks above 1gbps.

Figure 2 below illustrates the range of technologies currently used by consumers for broadband access.

Figure 2: OECD Broadband Subscribers per 100 inhabitants by Technology June 2006



[18] RF overlay uses wire as a broadcast medium, which makes it harder to undbundle: the technology choice is not regulatory neutral.

Source: OECD at http://www.oecd.org/dataoecd/50/49/37530046.xls

That urban/rural competition issue is the second of our contrasts. As broadband has been thus far largely a service offered by wired networks, using either coaxial cable, ADSL/SDSL and FTTx, the availability of sufficiently good quality wired networks has determined the ability for consumers and businesses to purchase broadband services. It may be obvious that the cost of wired infrastructure is very sensitive to the cost of deploying outside plant which is driven by density as a first order effect. Also, demand conditions are likely to be more favourable in urban areas (higher income, better educated, more back haul infrastructure available). We identify in the wireless chapter the possibilities for alternative futures involving wireless broadband, in particular deployment of WiMAX technology, but in the present, the urban availability of broadband is not replicated in many rural areas.

The wired/wireless distinction provides our focal point for addressing the urban/rural and symmetrical/asymmetrical divides. The greater the network capacity, the lesser should be the incentive to shape the IP traffic so that asymmetrical connections are offered (just as a 12-lane roadway can offer 6 lanes each way, whereas a 3 lane roadway must choose which traffic takes precedence with 2 or even 3 lanes). However, building such roads is expensive and depends on a network to provide the traffic at the end-points. We see enterprise broadband as the key early market segment in shaping the struggle between Mobile and Fixed and between Wireless and Wired access and service provision Enterprises may increasingly trade off portability for bandwidth. The lower data rates available through mobile/wireless will become decreasingly important by comparison with other service factors, some of which (e.g. reliability, security, immunity to crowding) may also be 'better' with fixed/wired. Bohlin et al state: "Fixed line…will act as a complementary backhaul long distance and feeder access network"[19]. 'Hot spot' architectures will rapidly bring 100Mbps peak rates within reach, particularly as for those wireless networks that employ fixed backhaul, that cost/price ratio declines rapidly. Dense high-speed wired coupled to upgrades in networking support for mobility will allow mobile edges for new architectures.

The following summary reflects our initial assessment of future developments in important functional areas.

Pricing and Cost

The cost issues concern: the balance of fixed and variable costs, investment in 'future proof' conduits; switches, etc. vs. cheaper or more immediately cost-efficient technology-specific alternatives; and the extent and management of joint, network and external costs[20]. On pricing, the key observation is that current provision supports a great profusion of charging models (from fixed to usage-, speed- or even content-dependent tariffs). €/Mbps is probably the appropriate metric, and the wide variance in costs of broadband in current markets may be expected to continue as new technology generations are deployed at different rates in different markets . Free connectivity is an option in many places for small enterprises (bundled with other services). Subscription rates may mirror the trajectory of per minute mobile costs, with steeply declining costs and bundling of total download/upload traffic (in the Terabyte/month range). Finally, a key

[19] Bohlin et al (2006) at 53.
[20] See Biggs, P. and Kelly, T. (2006) Broadband pricing strategies, 8 Info 6 at 3-14

joint issue is whether the technologies that follow the charging model will rest on common 'essential facilities' or some other architecture. Also, technologies can support new smart pricing streams to increase capacity utilisation, investment efficiency – the pricing model is the key link from technology to outcome.

Interoperability/Standards

We can expect to see increasing technological diversity: the old days of the single European 2G GSM standard are long gone. Cognitive/Software radio technology and home gateway boxes support considerable interoperability. In mobile 3G/4G networks, CDMA2000 and W-CDMA are both prevalent, but are not the only technologies in use. We examine the particular case study of WiMax and wireless alternatives to mobile WAN networks. In wired networks, we can anticipate pervasive IP giving way to native IP. We analyse in brief the case study of Next Generation Networks, where IMS and MPLS (Multiprotocol Label Switching) can create a 'single' traffic stream[21].

Power

Power consumption will remain a big impediment to portability, but will be addressed through progress with cogeneration and solar (for remote serving terminals), wider deployment of fuel cell technology and continued progress on increasing energy efficiency, including especially "energy-aware" application designs. This includes simply changing time to screen blank or resolution based on application in use to more exotic designs like modifying protocols based on the power environment. Bohlin et al state "Nanotechnology for building parts of handsets (especially with motive power) may be useful."[22] The use of polymer composites and other advances in battery life will aid mobility, as will improvements in solar and wind power[23].

Spectrum developments

We anticipate will retain further liberalization of spectrum with secondary trading and more unlicensed use, though reform may not be well coordinated internationally (at European or ITU levels). A key development is the use of 'package bidding' in new placements and secondary trading to allow flexible redefinition of spectrum (power, frequency, location) blocks to reflect technology and market conditions. This in turn will enhance incentives to develop agile technologies, new pricing models for services and even new configurations of content/communications offerings. Convergence of services and technologies will unbundle value chain to make many services frequency agile[24]. Implications include more efficient capacity utilisation, eroded 'silos' based on spectrum blocking, reduced distortion due to spectrum rights overhang. In turn, opening up the spectrum should encourage more jointly-useful innovation as opposed to

---

[21] See IETF (2006) MPLS Charter at http://www.ietf.org/html.charters/mpls-charter.html

[22] Bohlin (2006) supra n.16.

[23] For the larger enterprise, the increasing power needs of large server farms will be a significant cost issue: we note as an aside Google's use of the Oregon River to power their server farm and observe that such cost- and environmentally-efficient uses of larger power sources will become increasingly necessary and desirable. Government can play a role through incentive pricing in such uses.

[24] This "agility" arises at both the service and technology levels. At the service level, the traditional binding between specific RF frequencies and the services offered over them will be undone. For example, VoIP over fixed wireless broadband operating over multiple technologies in multiple bands will compete with 3G mobile services. In addition, as we discuss further below, innovative radio designs will allow radio devices to be frequency agile also.

spectrum-specific innovation or even "investment in incompatibility." Change will be incremental and for the near future, spectrum will most probably retain a mix of 'Command & Control', unlicensed, and licensed uses. The developing and developed worlds will develop at differing rates, but probably in similar or convergent directions. Slipstreaming and 'leapfrog' breakthrough by rural areas is quite possible given the disruptive nature of mesh networks. In the unlicensed domain, active RFID points the way to the 'Internet of Things', ambient and pervasive computing. At the moment these are low-power and low-bandwidth, but both are increasing rapidly and there is a pinch point regarding how they will be regulated/developed. Adequate reform ought to substantially lower the opportunity costs for accessing spectrum, supporting an explosion of innovation in wireless services.

Security

This is a growing problem as dependence on broadband (as a key element of the critical information infrastructure) grows and as ICT moves towards pervasive computing, and the 'Network of Things'[25]. There is an escalating arms race as attack and opportunistic behaviour become more sophisticated (SPAM, malware, DDoS, etc.)[26]. The objectives/requirements are also changing on both sides: on the attacking side, the evolution from unauthorised access to data corruption/exposure or access denial and on the defending side, the change in data collection/storage/processing locations (centralised or not), data exchange and transfer of liability among buyers, sellers and ISPs are all part of the evolutionary play being performed in the market/regulatory 'theatre'.

The responses are a mix of technological and 'soft' strategies, developed and deployed at both individual enterprise and wider levels. These include protected 'walled garden' environments, VPNs, etc. A potential loss of Internet openness and end-to-end connectivity is one potential casualty of security concerns. Another is privacy, which in some ways is the mirror of security. Again, there are differences between the developed and developing world, which are significant both in terms of the coherence and pace of technological development and because these worlds interact strongly. We identify some of the European Union's security policy challenges for broadband technology deployment in Chapter 4.

1.2 Structure of the Paper

The paper is structured as follows: In Chapter 2, we consider wired and wireless technologies; in Chapter 3 quality of service; in Chapter 4 we offer further research questions in the study of security, content and network regulation, and future broadband deployment. The examples deployed are predominantly though not exclusively European but the policy lessons are global. In the final chapter, we offer some conclusions for the role of government, and identify the further research questions which have arisen from this short survey of broadband technology trends.

---

[25] ITU Internet Reports (2005) The Internet of Things, at http://www.itu.int/osg/spu/publications/internetofthings/

[26] See Brown, I., Edwards L. and Marsden, C. (2006) Legal and institutional responses to Denial of Service Attacks, Communications Research Network/Department for Trade and Industry joint seminar on Spam/DDoS, 13 November, at http://www.communicationsresearch.net/events/article/default.aspx?objid=1464.

CHAPTER 2 Wired Broadband

In this short summary, we explain the key components in the development of copper (DSL), fibre (FTTx) and coaxial (DOCSIS3.0) development of fixed infrastructure. We briefly consider satellite (fixed in orbit rather than Low Earth Orbit (LEO) and powerline communications[27]. Our focus is on the market development path for high speed access in the 'local loop', from the local telephone exchange to the enterprise and home (SOHO). The reason for this focus is that the costs of broadband in the NGN 'core', the network, are already extremely high and in laboratories, optical fibre is producing even more extreme broadband speeds, while last-mile access networks present a bottleneck, both in terms of cost-recovery and available bandwidth.[28] Whereas the current late-twentieth century installed legacy networks often run at 655Mbps, with fibre optics and Dense Wavelength Division Mutliplexing (DWDM), which is widely deployed and has been so since 2000, the core network can run at 100-400Gbps. Fibre to the local exchange, which is widely but not universally deployed, may not become universal within the 2016 time horizon. The area in which regulatory policy problems will remain in pure speed terms is therefore the local loop.

Our focus in this chapter is broader, however. The ability to provide a multi-Mbps connection is a relatively simple technological challenge and may prove to be a logical marketing exercise[29]. The cost of the broadband connection is highly dependent on the range of support services that are mandated by law (as well as the demand-side priming by content and applications). In Chapter 3, we go on to consider the challenge of Quality of Service, and in Chapter 4, the cost of network security. In this chapter we focus on the cost of deployment: the roadworks and by-way costs of installing new plant, and the types of technologies that are emerging from laboratory testing and are being experimentally deployed. It is not unreasonable to suggest that one or more of such technologies may achieve broad market penetration

[27] Neither appears a particularly promising technology beyond existing uses including broadcasting and Global Positioning System uses. See Bohlin et al (2006) at 75 (satellite) and 106 (powerline).

[28] Utilization of last-mile links, which include more investment dedicated to single users/households is lower than what is achievable on "core" links, resulting in a cost-recovery challenge that helps explain why bandwidth is more limited in edge networks.

[29] The usage model we anticipate has important (and hard to change) implications for network we deploy (e.g., what is average/peak usage? how symmetric? open access? etc.). The marketing challenge will remain for any new/life changing good that is an "experience" good – we will not know what usage is until it is available and then changing it may be expensive. Policy may therefore favour flexible architectures.

within 10 years. However, we caution that, for instance, fixed wireless access (FWA) was offered as an alternative to the local loop in the early 1990s, and companies such as Rabbit and Dolphin in the UK, and others, failed to exploit the technology (though it was successful in Tokyo and Hong Kong, the latter branded as Rabbit). We focus in particular on wireless local loop for FTTx, a promising hybrid of wired and wireless technologies for less developed geographies in terms of FTTP or FTTH.

Regulation and interoperability play critical roles in next generations of broadband provision. In Chapter 4, we list the range of network and information security (NIS) requirements at European level that must be implemented in national law. They impose far from trivial costs on the network. They are in addition to existing costs for spam filtering, protection against Distributed Denial of Service (DDOS) attacks, phishing and other crimes that Internet Service Providers (ISPs) typically invest in to protect their subscribers from the worst excesses of IP traffic.

2.1 Copper Networks

The existing POTS network is typically twisted pair copper in the local loop. This can be upgraded using a Digital SLAM (DSLAM) in the local telephone exchange to offer ADSL. This technology can offer up to 20Mbps downloading speed or 2-4Mbps symmetrical speed. It can be further upgraded to later generations of technology, successively in terms of speed ADSL2, VDSL and VDSL2 with variations. These involve both more powerful DSLAMs and the siting of backhaul fire optical cable and the DSLAM itself closer to the cusomter premises (ideally in the street cabinet or even in the basement of the residential/enterprise's premises). At full capacity over short range, VDSL2 can provide 70-80Mbps through-put[30]. This permits multiple high definition video streams.

It is often overlooked that the maximum speed of a broadband connection is by no means the only variable in effective file transfer. First, the 'burstiness' (i.e. alternation) of the connection can depend on the network load, but is less important in downloading for delayed usage (e.g. downloading to a Personal Video Recorder PVR). Second, networks for distributing files are increasingly efficient: peer-to-peer networks take advantage of distributed file sharing and thus prevent overloading at one point in the network. Third, the compression of files, particularly video files, is improving rapidly, with latest generation MPEG4 and DivX codecs (compression-decompression) several times more powerful than previous generations. Fourth, the degree of Digital Rights Management (DRM) on the file may delay its route through the network if rules are set up to intercept content that is not 'authorised' to travel from one end-user to another. Fifth, the power of processors both in the network and at the end devices has increased so that disassembly and reassembly of digital packets is far more efficient than with previous generations of technology. For all these reasons, the simple 'peak' speed of a broadband connection is not in itself an indicator of the efficiency of file transfer. The following Table illustrates the developments in the efficiency of file transfer.

[30] Paltridge, Sam (2006) Internet Traffic Exchange, DSTI/ICCP/TISP(2005)11/FINAL, OECD: Paris.

Table: Technological Advances in End-user Devices

Technology nomenclature	Component	Cost-efficiency effect
Moore's Law	Microprocessor	Doubles every 18 months, e.g. from 2GHz to 4GHz
Metcalfe's Law	Network	Increases potential value of network by square of number of nodes
Disc Law	Storage – hard disk	Doubles storage cost-efficiency each year
Data packet transfer	Data compression	Increases: boosted by improved codecs e.g. DivX, RealPlayer, Windows Media
Gilder's Law	Transmission equipment	Bandwidth increases three times faster than microprocessor power – Moore's Law x3.
Fibre Law	Transmission network	Capacity doubles every nine months

Source: RAND Analysis

The increasing cost-efficiency of file distribution is predicted to continue, but the increased storage cost-efficiency of multimedia-ready PCs and PVRs is likely to be the biggest change in consumers' homes in 2011[31]. Ofcom provides a simplified version of the adoption curve shown in Figure 2 below, which illustrates the early stage of development of much digital content compared with technologies.

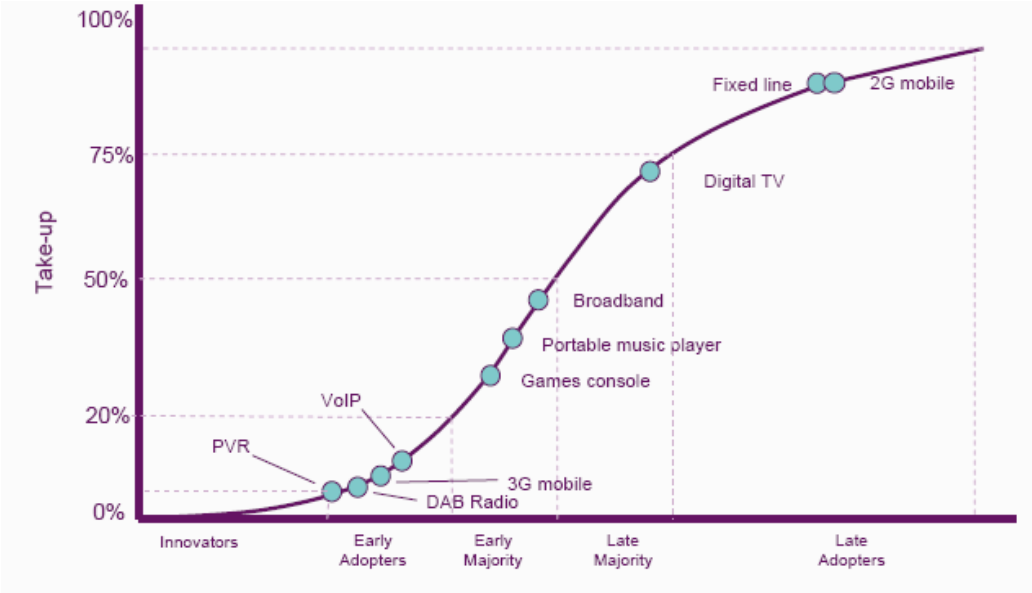


Figure 3: Composition of Current Technologies on the Adoption Curve

Source: Ofcom

Given the early stage of consumer adoption of so many technologies, we are cautious about the prospects for rapid demand-led upgrade beyond the copper loop, though we offer snapshots of interesting potential upgrade paths in the sections that follow.

2.2 Fibre Networks

The bandwidth advantages of photonics using fibre optic cable have been clear since the 1980s. The commercial deployment of such technologies outside research establishments and corporate Ethernet networks has been much slower, a 'textbook' example of the slow diffusion of broadband technologies. Demand studies over time have become more cautious and realistic about the prospects of widespread

[31] See for instance Analysys (2006) Sophisticated Broadband Services: Final Report for Department of Trade and Industry, Analysys, Cambridge.

deployment of fibre[32], with increased realisation that the cost of the fibre itself and the switching gear is trivial compared to other services such as roadworks for installation, billing, network resilience, security, regulation, content and applications and so on[33]. In June 2006, there were 6.3m fibre subscribers in Japan, with typically 100Mbps download/10Mbps upload capacity[34]. In Sweden there are 500,000 subscribers[35]. Italy's FastWeb is also a leader in Europe[36]. Nevertheless, the low penetration thus far of fibre in Europe should make one cautious at predictions that in a decade there will be 'fibre everywhere'[37].

McKeown illustrates the enormous potential for photonics to enhance capacity in networks, suggesting that integrated photonics is at the same stage in 2005 as integrated microprocessors in 1965. he explains that nanophotonics□ offers lower cost and lower power, with integration of optics and electronics and silicon optics (e.g. SiGemodulators). Further developments include optical packet switching, integrated optical processing, switching and wavelength conversion, and integrated optical packet buffers.[38] The potential exists to revolutionise the backhaul and router network, as well as the well-known effects of DWDM in creating much greater efficiency in the network backbone.

2.3 Cable Networks

European cable operators have in general been slow to upgrade to broadband, with exceptions including Denmark, Belgium, Estonia, Lithuania, the Netherlands and UK (the New Member States in general have more cable subscriptions relative to overall broadband than the EU-15, a common pattern where overall penetration is low)[39]. The 1980s attempts to introduce an All Fibre Network (AFN) were abandoned on cost grounds in favour of Hybrid Fibre Coaxial (HFC), which is the current standard. It can carry broadband at up to 25Mbps[40].

The US DOCSIS3.0 standard has the potential to offer fibre-matching speeds, as explained by Dave Burstein:

> "GPON can go 250 down, 125 up. Verizon … probably won't offer those speeds at the beginning, but the folks involved are confident

---

[32] A comprehensive exercise was undertaken by the Institute of Electrical and Electronic Engineers (IEEE) – see Camp, J. (ed)(2000) Special Issue, Info, Vol.2 Issue 2. The purpose was to construct scenarios for complete fibre coverage of the United States by 2005. All scenarios have proven wildly optimistic.

[33] See Labbe, M. (2005) Laying the Fibre: A Detailed Cost Analysis, Broadband Properties, April at www.broadbandproperties.com which looks at the US case. In Europe, see analysis posted at www.europeftthcouncil.com/

[34] See official government statistics at http://www.stat.go.jp/data/getujidb/zuhyou/002.xls

[35] Van de Woude, D.H. (2006) European (Muni) Fiber to the Home and Fiber backbone projects, mimeo. Copy available on request at dirkvanderwoude@gmail.com

[36] See European Foundation for the Improvement of Living and Working Conditions (2005) EMCC case studies: Industrial change in the telecommunications sector: FastWeb at http://www.emcc.eurofound.eu.int/publications/2005/ef0567enC5.pdf#search=%22fastweb%20milano%22

[37] See Yardley, Matt (2006) Fibre, fibre everywhere? Analysys, February, at http://www.analysys.com/default_acl.asp?Mode=article&iLeftArticle=2061&m=&n=

[38] McKeown Nick (2005) How Emerging Optical Technologies will affect the Future Internet, NSF Meeting, 5 Dec at http://find.isi.edu/presentation_files/Nick_McKeown-FIND%20Mtg%20Dec%202005.pdf

[39] See further Forfás (2005) Broadband Benchmarking Study, November 2005, Forfas: Dublin.

[40] See Bohlin et al (2006) at 89.

> it will be reliable. Dynamic bandwidth allocation means the 2.4 gig down/1.2 gig up is effectively shared, so that 99+% percent of the time any user needing speeds in the hundreds of megabits can access them. Many important technical issues, including interoperability, are making good progress in FSAN.
>
> "BPON can raise speeds to 100 down, 30 up using similar techniques bandwidth sharing techniques. Until recently, effectively shared. This is important because Verizon will have deployed between 7M and 9M lines of BPON before they have enough confidence to switch over to GPON. BPON is 622 down, 155 up, split up to 32 ways. That's considerably better than the low end DOCSIS 3.0 (160/120), and similar to the high end DOCSIS 3.0 (1 gig/100 meg, shared to probably hundreds of homes.)"[41]

(Note that Burstein's Verizon claims have been criticized as over-supportive of GPON/BPON technology and business projections.) There is therefore competition in the largest cable market between fibre offered by the telco, and cable companies. In the European market, where cable companies are generally loss-making and owned by US investors, the standards set in the US are likely to predominate.

2.4 Next Generation Networks

NGNs are being deployed across Europe in the period from 2007, with completion of migrations to all-IP networks scheduled for the period from 2009. The change to NGNs creates new opportunities for de- and co-regulation as well as new potential for incumbents to create bottlenecks in access[42]. For broadband technology deployment, the business case for both incumbents and competitor networks depends on their assessment of the various factors at play[43]. A recent OECD workshop focussed on these issues[44]. Only Japan, for instance, has completed the negotiation of the new Reference Interconnect Offer (RIO) for NGNs[45]. Tim Wright from British Telecom has illustrated the extent of the interoperability and standards challenges in NGN by reference to the 'iceberg' (an analogy he credits to Cable & Wireless), intended to illustrate how much interconnection depends on cooperation between industry parties[46].

---

[41] Burstein, D. (2006) What Verizon FIOS Can Do: 250/125 GPON, 100/40 BPON, Promise of Open Set Tops, DSL Prime Newsletter, 27 September.

[42] See Marsden, C. (2006) Next Generation Networks and the Last Mile Bottleneck: A Co-Regulatory Solution?, forthcoming in Telecoms Policy. There is very little non-technical academic literature on this subject doe to its novelty.

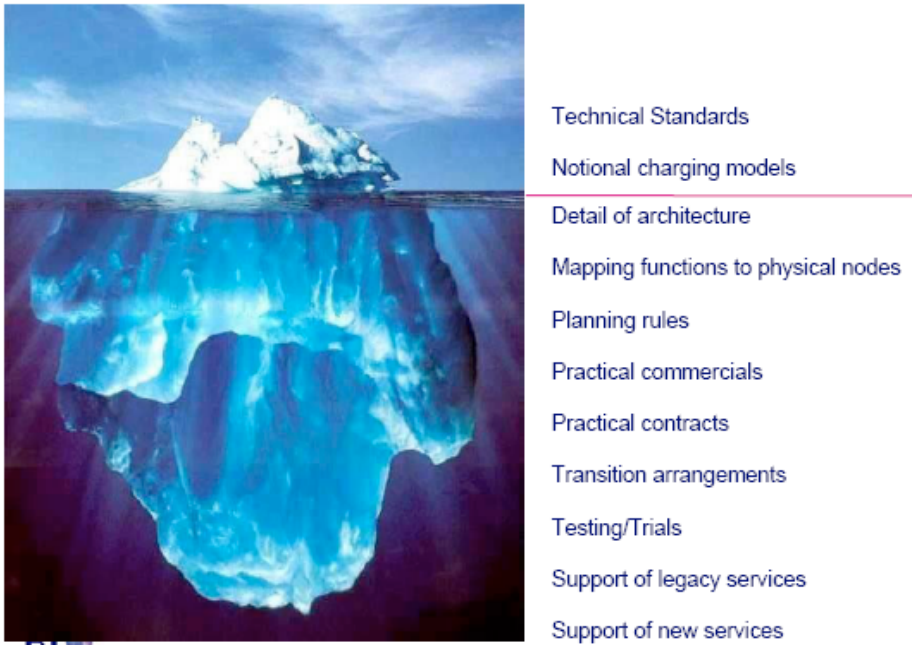
[43] Key feature here is whether future will entail locally owned last-mile shared infrastructure (muni fiber al a Stockholm) that could be shared with multiple providers so competition is not at last-mile but from first point of electronics and beyond.

[44] OECD Foresight Forum (2006) "Next Generation Networks: Evolution and Policy Considerations" 3 October 2006, at http://www.oecd.org/document/12/0,2340,en_2649_33703_37392780_1_1_1_1,00.html

[45] See Katagiri, Yoshihiro (2006) "Japanese interconnection policy on NGN" at http://www.oecd.org/dataoecd/6/52/37503176.pdf

[46] Wright Tim (2006) Next Generation Networks - the Interconnect Challenges, 13th CEPT Conference, 11-12 October 2006.

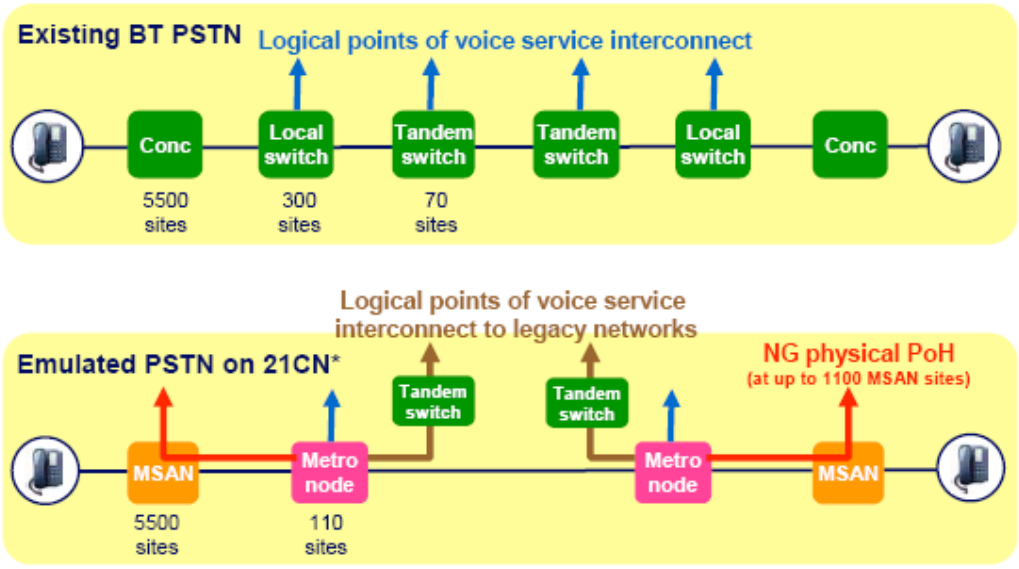
Figure 4: The Interconnection 'Iceberg' Showing Levels of Interoperability



Source: Wright (2006)

He has also illustrated the challenges to the existing interconnection regime of the 21CN, as shown in Figure 4 below.

Figure 5: Proposed Points of Interconnect for British Telecom (BT) 21CN NGN



Source: Wright (2006)

With 110 logical interconnect points, and 5500 local exchanges as Points of Handover, there is a substantially different network architecture for competitors to adjust their plans for.

2.5 Wireless Local Loop from FTTx

In countries and geographies without the medium term prospect of fibre in the local loop, an alternative which is made commercially available is Wireless Local Loop (WLL) offered at the point of fibre connection, for instance the local exchange. This offers the prospect of much higher

bitrates than WiMAX (see next chapter) because the WLL node also offers backhaul to the NGN network. Because the telco only has to supply fibre as far as the local exchange, it provides a much more cost-effective way of offering near-FTTx speeds without needing to invest in the 'last mile' wired local loop[47].

2.6 Conclusions: Fixed Wireless Potential and Constraints

Fixed wireless offers upgrade paths from current broadband to much greater speeds, which are already available in the core network but depend on upgrading the network to next Generation Networks. In the local loop bottleneck, the options for wired deployment are expensive and depend on anticipated returns on investment, which includes factors such as regulation, security, and the ability to discriminate.

[47] See for instance http://www-g.eng.cam.ac.uk/photonic_comms/pages/News/Light_reading.html

CHAPTER 3 Quality of Service and Network Deployment

The provision of unbundled DSL (a vertically disintegrated platform for service providers to add content/applications/services) at either wholesale or retail level will be considered by the regulation and competitive dynamics papers. However, it is important to consider the *technological implications* of the various competitive and regulatory options. Return on investment is the key to network operators' decisions to invest in NGNs, and a critical part of that decision is the consideration of whether the network is offered as a non-discriminating wholesale or retail network, or a 'walled garden'. These decisions, whether taken as a competitive strategy by the operator or mandated by the regulator, are critical to network architecture. In brief: networks can build for pure speed or for safety/convenience/privacy, and there is a critical cost trade-off between these two poles. Consider the mobile telephony network: it offers almost complete mobility (seamless except on urban public transport), filters out spam and viruses, and provides vertically integrated content, applications and services that are robustly matched to the platform. It also currently operates at sub-1Mbps speeds. By contrast, many wired operators offer enterprises Gbps Ethernet connections to their premises. This may appear a crude comparison, but it illustrates the point that strategy determines technology, and not vice versa.

3.1 Regulating for Quality of Service (QoS)

Governments mandate many QoS standards for operators, and many more are contractually required within Service Level Agreements (SLAs) between operators, and from operator to end-customer. SLAs typically offer a market-based equivalent to government requirements for network resiliency and emergency management: the need to keep the service running at capacity and guaranteeing to repair faults in good time. However, beyond these basic requirements, governments also set targets for: universal service; number portability between carriers; emergency telephone number availability; power redundancy to maintain the system in case of a general electricity grid fault; billing system accuracy; customer service response; independent arbitration of disputes. At a local level, cable franchises are often required to offer a percentage of their channels for designated programming, and all local roadworks are subject to various requirements of repair, compensation and by-way legislation. These are far greater costs than the comparatively trivial costs of running a broadband network at several Gbps.

Recent legislation has increased those regulatory costs on networks. In Appendix 1, we list some of the many security and police requirements for networks. Here we offer a different example, which will also impose significant costs on network design from about 2009 and throughout the period to 2016.

3.1.1 Network Monitoring of Video and Other Traffic Types

Consider the European Commission proposals for revision of the 'Television Without frontiers' (TVWF) Directive to require co-regulatory schemes to be instituted to monitor and prevent potentially harmful commercial video files from being distributed over the Internet. Enforcement can only be undertaken successfully by the content host. More effective policing of content by this host is required for video content transported onto their networks. This requires a type of control to identify the content as it enters the network: a type of 'walled garden'[48]. Note that (with relative technical ease) users can encrypt their video content and thus evade the more basic types of policing carried out by the network provider[49].

Network providers might be expected to argue that such a new control strategy would require extensive and expensive upgrades to their systems. While this is partially true, there are other reasons why providers may have this capability already:

1. A type of traffic inspection is required for government law enforcement and security purposes.
2. Network providers already provide filters against the more obvious types of 'spam' – unsolicited commercial communications.
3. Network providers cooperate with national security agencies in tracing potential terrorist activities via their file transfers on the Internet.
4. Network providers can trace non-encrypted Voice over Internet Protocol (VoIP) communications and block these packets.
5. Network providers are increasingly adopting Quality of Service architectures for their networks in order to prevent users from over-straining the network at times of peak usage, and in order to charge content owners for value-added high-volume services such as video files.

These new developments allow network providers to block video file transfer, or more appropriately to charge the users a carriage fee for sending such large files. This is the solution adopted by mobile operators and some network providers, and is generally termed a 'walled garden' to denote the isolation of content on the network from other content on the wider Internet. We consider the cost and technology case for this policy below.

---

[48] The Chinese government requires this of its network providers, although using much simpler technologies. See Clayton, R., Murdoch, S.J. and Watson, R.N.M. (2006) 'Ignoring the Great Firewall of China', paper presented to the Sixth Workshop on Privacy Enhancing Technologies, Cambridge, UK, 28 June, at: http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf

[49] For an excellent primer, see Felten, E. (2006) 'Nuts and Bolts of Net Neutrality', 11 July, at http://itpolicy.princeton.edu/pub/neutrality.pdf

3.2 Content Discrimination and Charging

If innovation is typically both user-distributed and user-driven, the implications are that innovation is encouraged by interoperability and open access: in general, ensuring that content can be shared freely between those users. This view is in some conflict with content and network owners' need to be recompensed for their services and has led to an animated debate in the USA. In 1999, Lemley and Lessig argued against permitting cable companies to discriminate between Internet traffic[50]. Their claim was that innovation at the edge of the network is opposed by traditional media and network businesses, as it makes business cases based on controlling distribution bottlenecks redundant: where there is peer sharing, there is less opportunity for traditional bottlenecks and therefore control of revenues. However, the inverse also applies: without some means to secure revenues for the increased bandwidth necessary for Web2.0 type applications to flourish, do network operators have an incentive to upgrade? As Ed Whitacre famously stated:

> "The Internet can't be free in that sense, because we and the cable companies have made an investment and for a Google or Yahoo! or Vonage or anybody to expect to use these pipes [for] free is nuts!"[51]

Content charging relies on a type of Quality of Service for the Internet, enabling network providers to discriminate (in Lessig's terms, to regulate) between packets. The standards body for 3G (third generation) mobile telephony, 3GPP, has been working since 2000 on a set of standards called IMS (IP Multimedia Subsystem)[52]. This is an operator-friendly environment intended to generate new revenue via deep-packet inspection. Fixed-line carriers and equipment vendors have created the 'IPsphere', a new set of standards for network intercession in IP application flows[53]. Both sets of standards support the ability to filter and censor by file type on the Internet. This enables the carrier to discriminate, to decide which content to delay and which to permit to travel at normal speeds to the end-user. As Cisco standards expert John Waclawsky puts it:

---

[50] This testimony to the Federal Communications Commission (FCC) was later published as Lemley, M.A. and Lessig, L., 'The End of End-to-end: Preserving the Architecture of the Internet in the Broadband Era' (2001) 48 UCLA Law Review 925. Other notable contributions to the debate include: Wu, T. (2003) 'Network Neutrality and Broadband Discrimination', Journal of Telecommunications and High Technology 2: at p. 141; Yu, C. (2004) 'Would Mandating Network Broadband Neutrality Help or Hurt Competition? A Comment on the End-to-end Debate', Journal of Telecommunications and High Technology 3(2), at p. 23; Farrell, J. and Wesier, P.J. (2003) 'Modularity, Vertical Integration, and Open Access Policies: Toward a Convergence of Antitrust and Regulation in the Internet Age', Department of Economics UCB Paper E02-325. Berkeley: CA: University of California at Berkeley; Woroch, G.A., Open Access Rules and the Broadband Race' (2002) 3 Law Review of Michigan State University–Detroit College of Law 1, at pp. 1–24 .

[51] Business Week International Online Extra (2005) 'At SBC It's All About Scale and Scope', 7 November, at: http://www.businessweek.com/@@n34h*IUQu7KtOwgA/magazine/content/05_45/b3958092.htm

[52] See Wadawsky, J. (2005) 'IMS 101: What You Need to Know Now', at: http://www.bcr.com/carriers/public_networks/ims_101_what_need_know_now_2005061514.htm

[53] See IPSphere (2006) 'Creating a Commercially Sustainable Framework for IP Services Realizing Next Generation Revenues', IPsphere Forum Work Program Committee Version 1b.0, May, at: http://www.ipsphereforum.org/home/IPsphere_CommercialPrimerExec050806.pdf

> "This is the emerging, consensus view: That IMS will let broadband industry vendors and operators put a control layer and a cash register over the Internet and creatively charge for it."[54]

The interoperability debate is broader than simply an Internet access debate, as it affects innovation in software – indeed, the origin of the argument lies with software industry disputes over interoperability, an argument captured by Lessig in his contribution to the *Microsoft* litigation[55]. The debate has centred on the legislation in the US Senate[56] and Congress permitting US network operators to discriminate between the Internet traffic that they carry. In Europe, the debate has developed more slowly, and the new proposed Electronic Communications package does not propose so-called 'net neutrality' provisions, instead continuing to permit national regulators to make policy. The European Commission states in full:

> "In Europe the regulatory framework allows operators to offer different services to different customer groups, but does not allow those who are in a dominant position to discriminate between customers in similar circumstances. However, there is a risk that, in some situations, the quality of service could degrade to unacceptably low levels. It is therefore proposed to give National Regulatory Authorities (NRAs) the power to set minimum quality levels for network transmission services in an next-generation network environment based on technical standards identified at EU level. The existing provisions for NRAs to impose obligations on operators with significant market power, and the powers for NRAs to address access and interconnection issues could be used to prevent any blocking of information society services, or degradation in the quality of transmission of electronic communication services for third parties, and to impose appropriate interoperability requirements."[57].

The European debate does not discuss legislative reform, as in the US. It is a question of forensic examination of any potential discrimination which can be pursued – subject to regulatory will – under the current legislation. Nor is it restricted (at least in theory) to dominant (Significant Market Power) actors. The blocking of Skye's VoIP product is at least in theory actionable, as is that of many ISPs in blocking BitTorrent for what are claimed to be legitimate security concerns. We return to this issue in Chapter 4. (Protection of intellectual property rights by DRM has too broad a scope for this short paper.)

3.3 Conclusions: Business Cases for Technology to Aid Traffic Discrimination

There are incentives for network providers to police the traffic by type, if not by content[58]. Therefore it enables the network providers, many of whom also operate their own proprietary applications, to charge a

---

[54] Wadawsky (2005) supra.
[55] Lessig, L. (1999) Brief as Amicus Curiae *U.S.* v. *Microsoft*, 65 F.Supp.2d 1 (DDC. 1999), at: http://cyber.law.harvard.edu/works/lessig/AB/abd9.doc.html
[56] See Communications, Consumer's Choice, and Broadband Deployment Act of 2006, at: http://thomas.loc.gov/cgi-bin/bdquery/z?d109:SN02686:@@@L&summ2=m&
[57] See European Commission (2006) 'Staff Working Document', 28 June, at: http://ec.europa.eu/comm/avpolicy/reg/tvwf/modernisation/consultation_2005/index_en.htm, at section 6.4, Net Neutrality.
[58] This permits some enforcement potential for the AVMS, in that unencrypted video files can be monitored. It also permits network providers to charge independent content owners for carriage of their video files over the network.

different price to non-affiliated content owners than affiliated owners. This differential pricing could make the profitable operation of non-affiliated providers more difficult. On that basis, the 'walled garden' might become the more successful business model. That model makes regulation much easier to enforce, but also prevents some of the interoperability and open access for users that is held to lead to much Web2.0 innovation for businesses. (We note that encryption and other technologies mean that no 'walled garden' would be entirely closed.) It is not the aim of this report to provide the 'right' answer in the complex trade-off between, on the one hand, regulated 'walled garden' networks and affiliated content providers, and on the other, open interoperable but only self-regulated Internet access.

Raising the issue of business cases for broadband filtering technologies illustrates our main conclusion from the study of broadband technologies: it is not the speed of broadband which is a challenge, but the cost and quality of the applications and content provided over that broadband network. In the following chapter, we consider security policy challenges.

CHAPTER 4 European Network and Information Security Law and Policy

4.1 Security and Other Legitimate Aims, or Smokescreens

Information systems are increasingly important to the efficient operation of government, corporations and society in general, but with that importance comes an increasing risk of information security breaches compounded by their networked nature. That makes effective information security a public policy issue of far broader impact than technical information technology (IT) policy. Network and Information Security (NIS)[59] policy making and investment have evolved rapidly, especially since 1999. This evolution has been punctuated at certain points where the necessity of adequate or mature NIS policy has been sharply emphasised by vulnerability to attack or shocks:

- The 'Millennium Bug' or Y2K programme of 1997-9, which led to a complete inventory of computing inside large organisations, often for the first time since the deployment of the enterprise Personal Computer (PC) in the mid-1980s;
- Denial of Service (DoS) attacks, beginning in 2001 against Yahoo! and eBay;
- Business continuity planning and counter-terrorism policy in the wake of the attacks of September 11th 2001;
- Corporate responses to the increasing financial returns for attackers (for example the growth of 'phishing' and the 2004-5 cyber-blackmailing cases against gambling websites).

There has been little rigorous independent research, though legislation, policy, government spending and corporate response in the field of information security have been examined by for instance the Organisation for Economic Cooperation and Development (OECD)[60] and the European Commission (DDSI project)[61].

---

59 Definitions vary. Here we use the working definition of Commissioner Erkki Liikanen. "What do we understand by NIS? I give you the following definition: "it is about ensuring 'the ability of a network or an information system to resist, with a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of data and the related services offered by or accessible via these networks and information systems'." See http://europa.eu.int/rapid/pressReleasesAction.do?reference=SPEECH/03/65&format=HTML&aged=0&language=EN&guiLanguage=en

See further COM(2003) 63 establishing a broad definition for the working of ENISA.

60 See OECD (2005) The Promotion Of A Culture Of Security For Information Systems And Networks In OECD Countries DSTI/ICCP/REG(2005)1/FINAL of 16 December 2005 at http://www.oecd.org/dataoecd/16/27/35884541.pdf

61 The 2001-2 Dependability Development Support Initiative at http://www.ddsi.org/DDSI-F/main-fs.htm

4.2 UK Law on DOS and Distributed DOS (DDOS)

Computer Misuse Act 1990 Amendments

The Computer Misuse Act (CMA) was enacted in 1990. It remains the primary piece of UK legislation focusing on the misuse of computer systems. It covers crimes such as hacking (s 1) and the deliberate spreading (not writing) of viruses (s 3). These crimes are rendered legally as, respectively, "unauthorised access to" and "unauthorised modification of" computer systems. In 2004, Members of Parliament – specifically, the All-Party Internet Group (APIG) – began a review of the CMA, on the basis that this legislation was created before the emergence of the Internet and therefore required updating. The Act was seen to focus too much on standalone computers and not enough on computer networks. In addition some of the definitions used in the 1990 Act need updating.

The final report outlined several recommendations to the government for changes to the CMA. In March 2005, APIG called for amendments to the CMA , in particular to address the threat from denial-of-service (DOS) attacks. It was felt to be bot atcall clear if the CMA covered all types of DOS attacks. An updated version of the CMA could be of greater benefit if it combined computer crime regulations relevant to standalone and network situations. Furthermore, the sanctions of the CMA were seen as outdated and an inadequate deterrent to cyber-criminals.

Criminalising DOS

As the APIG report noted, one of the problems with deciding if the CMA covered DoS was that the analysis of the differences between DoS and DDOS attacks has in many cases been muddy. In "plain" or "vanilla" DoS, the only computer system affected is usually the target. The most obvious offence committed might seem to be unauthorised access. Yet as various commentators have pointed out, it was difficult to see the access that is perpetrated in DoS, harmful though it is in bulk, as "unauthorised". Websites that were not protected by passwords or other types of authentication were regarded as impliedly authorising, indeed encouraging, third parties to "visit"--that is, make page and file requests. In the case of distributed DOS – DDOS - almost certainly the zombie machines used to mount the DDOS attack will have been infected by viruses so a s 3 charge will be viable. However it seemed desirable to APIG to have one charge which could be prosecuted in all cases of DOS-style attacks whether mounted as straightforward attacks from one machine (DOS), or using enslaved networks of infected machines (DDOS).Partly as a result, attempts to criminalise both DOS and DDOS have focused mainly on s 3 of the CMA. This raised two main issues: modification, and, as already noted above, authorisation, or , what is "unauthorised"? These are discussed below.

The UK Home Office then tabled proposals in the Police and Criminal Justice Bill 2006 to adjust the CMA to make Denial of Service explicitly illegal and also to increase the maximum penalty for some offences to ten years. The Bill received the Royal Assent on 8 November 2006. First, the Act doubles the maximum jail sentence for hacking into computer systems from five years to ten years, a provision that will classify hacking as a more serious offence and make it easier to extradite computer crime suspects from overseas. Second, the Act introduces a substantive offense of denial of service by the indirect means of amending s 3 of the Computer Misuse Act (CMA). Section 3 in

original form, as noted above, was designed to criminalise the spreading and transmission of viruses. It required "*unauthorised modification*" of the contents of the computer targeted for criminal liability to be imposed.

4.3 European Law

The European Union (EU) is the world's largest free trade area, and all twenty-five Member States must implement European law. Failing implementation, European law can in certain circumstances take direct effect despite the lack of national law. Therefore much over-arching NIS legislation and policy takes place at European level.

Table : Summary of national legislation and European law implementing NIS[62]

Jurisdiction	Privacy Law	Electronic Privacy Law	Electronic Commerce Law[63]	Cyber Crime Law[64]
European Union	Data Protection Directive 95/46 of 24 November 1995	Directive 2002/58/EC repeals Directive 97/66/EC 15 December 1997, Data Retention Directive 2006 of 21 February	Electronic Signatures: Directive 99/93 of 13 December 1999 Electronic Commerce: Directive 2000/31 of 8 June 2000	Communications from European Commission but main law is 2001 Council of Europe Convention on Cybercrime
United Kingdom	Data Protection Act 1998	Regulation of Investigatory Powers Act 2000, Privacy and Electronic Communications Regulations 2003	Electronic Communications Act 2000, Electronic Signature Regulations 2002, E-Commerce Regulations 2002	Computer Misuse Act 1990
Germany	Federal Data Protection Law(BDSG) last amended 2001; G-10 law applies to communications secrecy	Information and Communication Services Act 1997, Telecommunications Act 2004 (Tele kommunikationsgesetz-TKG) last amended 14/03/2005	Digital Signature Law 2001	Penal Code Sections: 202a: Data Espionage 303a: Alteration of Data 303b: Computer Sabotage
France	Information Technology and Liberty Act (Loi Informatique et Libertés) 1978	Law 2004-801 of 6 August 2004 relating to the Protection of Data Subjects as Regards the Processing of Personal Data	E-Signature Law: Decree No. 2001-272, 30 March 2001 in accordance with article 1316-4 in the civil code and related to electronic signatures Law n°2004-575 of 21 June 2004 of Confidence in the Digital Economy	Godfrain Act 1988. Penal Code Chapter 3, Articles 323-1 through 323-4: Attacks on Systems for Automated Data Processing

62 For a current survey, see Mitrakas, Andreas (2006) Information security and law in Europe: Risks checked? 15:1 Information Communications Technology Law March at 33-53.

63A useful source of e-banking legislation in English is http://rechtsinformatik.jura.uni-sb.de/cbl/cbl-statutes.php

64 All countries in the Table have signed the Council of Europe Cyber Crime Convention.

National legislation is increasingly[65] a required transposition of European Directives into national law, though acute differences in interpretation can arise. Thirty per cent of legal proceedings brought by the European Commission against Member States for late or inaccurate transposition of European Directives into national law are brought against two countries: France and Italy[66].

The implications of federal structures and constitutional constraints should be mentioned. Relations between the EU and the Member States are not directly comparable to those between US federal and state governments. An important difference is constitutional. Whereas the United States Constitution establishes citizen protections at federal level directly enforceable by the Supreme Court, Europe has no such overall constitution and national 'Supreme Court' actions can overturn European legislation resulting in legal impasse. European law trumps national law where economic rather than other human rights (such as defence, taxation, crime prevention and privacy) are concerned.

There is evidence of harmonisation among countries based on both common European legislation and strong evidence of cooperation in for instance police and CERT[67] activities. The extent to which this harmonisation resulted in convergence of national policies depended critically on:

- Whether national political responses to specific NIS problems[68] produced strong national legal and policy differences; and
- Whether pan-European policy preceded national response.

Areas with pre-existing and strong national NIS policy frameworks were most associated with interviewee reports of strong national divergence from the European 'standard'. An example is data protection. French and German legislation and national regulators date from the 1970s, while the UK and Italy adopted later and therefore had greater need to raise protection levels in response to the agreed European 'standard' (the 1995 Data Protection Directive[69]). European law sets high standards for data protection, arguably higher those that in the United States.

National responses to cybercrime date from the period around 1990 and also show significant legislative and policing developments that pre-date the European response (ENISA, the European Network and Information Security Agency, was only founded in 2005). In criminal law, pre-existing national legislation combined with a European cooperative police force (Europol) led to harmonisation rather than convergence. In all these cases, European legislation came after national legislative and institutional arrangements, and national lawmakers had substantial initial room for independent policy formation. In telecoms legislation, an area of longstanding European convergence, the Data Retention Directive of 2006 which we consider

65 Over half of all UK legislation is now transposition of European legislation.

66 See the 2003 (12th) and 2005 (14th) Implementation Scorecards: http://europa.eu.int/comm/internal_market/score/docs/score14bis/scoreboard14bis_en.pdf and http://europa.eu.int/comm/internal_market/smn/smn32/a4_en.htm#note1

67 Computer Emergency Response Team.

68 Including data protection failures and prevalence of viruses and other computer crimes.

69 National data protection agencies have a permanent joint working group, and are required to implement as uniformly as possible the Data Protection Directives (notably Directive 95/46). The European institutions are also required by law to consider the Opinions issued on prospective legislation by the European Data Protection Supervisor, established in 2002.

below signalled a greater convergence between national regimes. The very late establishment of ENISA as the central NIS coordination mechanism indicates a desire by Member States to maintain existing national institutional arrangements in their current form.

4.4 Data Retention Directive

European institutions gave legal form on 21st February 2006 to the Data Retention Directive, which requires intermediaries in public communications networks to retain data on telephony, Internet, email and Instant Message communications for set time periods, imposing significant data storage costs. The implementation of this Directive in national law is not due until August 2007, and will be delayed in several countries by the usual constitutional and parliamentary procedural lapses associated with transposition of European law into national law. Therefore this Directive will not begin to impose costs on corporate actors until 2007-2008.

The Data Retention Directive relating to telecoms networks, and therefore NIS, was approved by ministers in Brussels on 21 February 2006, concluding a lengthy debate inside and outside EU institutions.[70] The Data Retention Directive was tabled after the Madrid bombings in March 2004 and then fast-tracked under the British EU Presidency after the London Underground attacks of 7th July 2005. Britain, France and Sweden have stressed the need to retain data in order to trace terrorists using modern technology. According to the Directive, Member States will oblige communications providers to store citizens' phone call data for six to twenty-four months, but the Directive does not stipulate a maximum time period: some Member States want longer storage periods. The data would only detail the caller and receiver's numbers, not the actual conversations themselves, while so-called failed calls - calls that do not get through - will not be covered. EU countries have eighteen months to implement the rules.

New legislation may only be passed into law following a mandatory Impact Assessment since 2003, as part of the Better Regulation agenda of the European institutions. Therefore, laws imposing costs on European businesses to provide rights for government or citizens to access data for security or data protection purposes, must be costed and justified. The new rules for implementing Directives mean that a publicly available Impact Assessment was issued for the Data Retention Directive. It is an exemplar of the new approach to European legislation that will be adopted in future for legislative proposals. ETNO (the European Association of Telecommunications Network Operators) indicated that for a one year retention period, costs would be above €150m for a large network and service provider (more than €100m for retention of traffic data for software, server, security, and at least €50m for annual overhead expense). [71]

The European Commission has indicated that: “Indirect benefits could thus include a possible reduction in cybercrime, and in any case a situation which is not worse than the current one for law enforcement efficiency. It will therefore be difficult to assess indirect costs before some years (sic) of implementation of the Directive, in 2010-12.” The

[70] Unofficial text available at http://register.consilium.eu.int/pdf/en/05/st03/st03677.en05.pdf

[71] http://europa.eu.int/comm/secretariat_general/impact/docs/ia_2005_3/COMM_PDF_SEC_2005_1131_1_EN_DOCUMENTDETRAVAIL.pdf

cost-benefit analysis of NIS legislation compares the long-term effect of legislation in countering crime versus increased costs for telecoms operators in implementing measures to comply with the law. In this case, the costs and benefits were not submitted to an independent evaluation for the impact assessment72 . Therefore the trade-offs were not considered independently.

Eurostat conducts regular surveys of pan-European e-commerce and the assessment of Internet use and security breaches. The latest such survey was conducted in 2004 and published in 2005, demonstrating that both attacks and poor levels of business response has been most apparent in the SME sector, and more so in less mature markets in Eastern and Southern Europe than in the north and west[73].

4.5 European Legislative Instruments

The following Directives, Regulations and Communications implement network information security policy[74] at the EU level.

Data Protection Directive: Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.75 This is the main law giving Member States responsiblities and citizens data protection rights against corporate actors. This European law sets a high standard for data protection, arguably higher than that in the United States. National data protection agencies have a permanent joint working group (the Article 29 Working Group), and are required to implement as uniformly as possible the Directive. The European institutions are also required by law to consider the Opinions issued on prospective legislation by the European Data Protection Supervisor, established in 2002.

There are two Directives which establish the criteria for pan-European e-commerce passed in 1999-2000: Electronic Signatures Directive: Directive 99/93/EC of 13 December 1999 on a Community framework for electronic signatures[76] and E-Commerce Directive: Directive 2000/31/EC of 8 June 2000 on certain legal aspects of

---

72See http://www.europarl.eu.int/omk/sipade3?PUBREF=-//EP//NONSGML+WQ+E-2006-1131+0+DOC+WORD+V0//EN&L=EN&LEVEL=2&NAV=S&LSTDOC=Y

73 See http://epp.€tat.cec.eu.int/cache/ITY_OFFPUB/KS-NP-05-025/EN/KS-NP-05-025-EN.PDF

74 Definitions vary. Here we use the working definition of Commissioner Erkki Liikanen. “What do we understand by NIS? I give you the following definition: "it is about ensuring 'the ability of a network or an information system to resist, with a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of data and the related services offered by or accessible via these networks and information systems'.” See http://europa.eu.int/rapid/pressReleasesAction.do?reference=SPEECH/03/65&format=HTML&aged=0&language=EN&guiLanguage=en
See further COM(2003) 63 establishing a broad definition for the working of ENISA.

75 Directive 95/46/EC available at: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett

76 Directive 1999/93/EC available at: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31999L0093&model=guichett

information society services, in particular electronic commerce, in the Internal Market.[77]

An entire package of Directives were passed together in 2002 to improve the provision of electronic communication services, of direct impact essentially on telecoms operators, including the Access Directive on access to, and interconnection of, electronic communications networks and associated facilities[78], and the Authorisation Directive on the authorisation of electronic communications networks and services[79]. Below we detail the most relevant of the Directives.

Framework Directive: Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services lays down the tasks of national regulatory authorities, which include cooperating with each other and the Commission in a transparent manner to ensure the development of consistent regulatory practice, contributing to ensuring a high level of protection of personal data and privacy, and ensuring that the integrity and security of public communications networks are ensured.80

Directive on privacy and electronic communications: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector81 includes measures intended to prevent the sending of unsolicited electronic communications within Europe (so-called 'spam'). It has been supplemented by the 2004 Communication82 on unsolicited commercial communications or 'spam'83 .

Council of Europe Convention on Cyber-crime: One of the main international legislative instruments relevant in the scope of Europe-wide NIS activities is the Council of Europe Convention on Cyber-crime. The final text of this was agreed on 23 November 2001 and the Convention is open for signature by Council of Europe Member States (EU Member States plus fifteen other countries) and those non-Member States that participated in its drafting (including the United States). It is also open for accession by other non-Member States. The Convention is regarded as one of the most comprehensive documents on cyber-crime available. Substantively, it focuses on efforts to outline common definitions for crimes relating to computers and also measures to

---

77 Directive 2000/31/EC available at: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000L0031&model=guichett

78 Directive 2002/19/EC available at: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0019&model=guichett

79 Directive 2002/20/EC available at: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0020&model=guichett

80 Directive 2002/21/EC available at: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0021&model=guichett

81 Directive 2002/58/EC available at: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0058&model=guichett

82 Communications from the Commission, and Resolutions of the Council are not European legislation and therefore non-binding on Member States but have important 'signalling' effects on Member States and companies, and therefore are termed 'soft law'

83 Communication (COM/2004/0028) available at: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=52004DC0028&model=guichett

encourage international co-operation. The Convention entered into Force on July 1 2004.84 A further Protocol was signed on 28 January 2003 but has not yet entered into force85 .

4.6 European Policy Instruments and Developments

European Council Framework Decision on Attacks against Information Systems: The European Council Framework Decision on Attacks against Information Systems was adopted on 24 February 2005. Its objective is 'to improve cooperation between judicial and other competent authorities, through approximating rules on criminal law in the Member States in the area of attacks against information systems'. The Framework Decision indicates that attacks against information and computer systems are a tangible and dangerous threat that requires an effective response. The Framework Decision and the Cyber-crime Convention synchronise definitions.

The eEurope Action Plan is the current strategy in use to meet the goals of the 2000 Lisbon summit, relating to making the EU the most competitive dynamic knowledge based economy by 2010.

eEurope 2005: In 2002 at the European Council meeting in Seville, the eEurope 2005 Action Plan was launched. The e-Europe resolution published by the European Council in January 2003 endorsed the eEurope Action Plan and emphasised the importance of further progress to keep the development of the e-Economy as a priority for the European policy agenda. The resolution stressed as a priority the importance of ensuring the "appropriate security of networks and of the information transmitted through them for individuals, businesses and administrations and other organisations." Member States were to help in achieving the objectives of the Action Plan, promote network security and promote e-Business, taking into account specific national contexts.86

The e-Europe 2005 Action Plan aimed to "develop modern public services and a dynamic environment for e-business through widespread availability of broadband access at competitive prices and a secure information infrastructure." In detail, the eEurope 2005 Action Plan explicitly stated the importance of NIS as one of eEurope's six policy priorities: "Until security issues are addressed, therefore full development of the information society can not take place. Security is therefore a key component of the Commission's vision for the Next Generation Internet."87

---

84 Due to its article 36, which contains the conditions for entry into force. It specifies that the Convention should first be ratified by five States, including three Member States of the Council of Europe. The Convention would then enter into force on the first day of the month following the expiration of a three month period after the fifth ratification. This condition was fulfilled with Lithuania's ratification on 18 March 2004, triggering the entry into force on 1 July 2004.

85 Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems CETS No.: 189 at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=10/02/05&CL=ENG

86 http://europa.eu.int/information_society/eeurope/2005/doc/all_about/resolution.pdf

87 eEurope 2005 Action Plan: All About Security available at: http://europa.eu.int/information_society/eeurope/2005/all_about/security/index_en.htm

Efforts at overall policy development in the area of security also came under scrutiny in the eEurope 2005 Mid Term Review. Under the heading of "Meeting the objective of a faster and more secure Internet for all", the eEurope 2005 Strategy was found to require more effort to encourage development of formal information security policies amongst businesses which could have a negative influence on trust on the Internet by dissuading people from buying online. eEurope 2005 indicated that security was not just a technological issue, but was more about human behaviour and knowledge of threats and remedies. A number of policy areas were identified as being important for trust and security: privacy; industrial policy; international trade; citizens' rights; law enforcement; defence. The need to adopt a holistic approach at the European and global level was also identified. eEurope 2005 signalled the intention to pursue specific NIS policies at European and Member State level, focussing on improving NIS robustness.

CHAPTER 5 Conclusion: The Perfect Storm?

I have in this report laid out the type of cost-benefit decisions that are likely to influence the deployment of next-generation wired and wireless broadband. I have focussed in particular on the incentives and disincentives in security and Quality of Service in fixed line networks. I finally note that technology developments will depend on modelling the incentive structure. This can be implemented using game theory: "We need to elevate incentives to a first-order concern. We are at the start of that journey. Challenges and opportunities ahead include truly addressing incentives in designs."[88]

[88] Afergan, Mike (2005) Using Game Theory to Develop Network Architecture, at http://find.isi.edu/presentation_files/Mike_Afergan-FIND-preso.pdf