Rt Hon ALUN MICHAEL JP MP
HOUSE OF COMMONS
LONDON SW1A 0AA
E-MAIL: alunmichaelmp@parliament.uk
TEL: 020 7219 5980
Mob: 07768 883324

Tackling crime and achieving confiden in the on-line wor

Advance note for the Parliament & Internet Conference 18th October 2007

The Internet provides almost unlimited opportunities for communication and enterprise – but it also provides massive opportunities for exploitation, crime and nuisance. Public confidence is fragile – and growth in use of the Internet depends on public confidence. The question "who governs the Internet ?" needs to be answered, along with the question "who will protect the public ?" These separate questions are linked – and piecemeal solutions will not work

The "governance" issue can be dealt with through the partnership approach proposed in this paper. Neither of the alternatives (leave things as they are, with no genuine accountability, or establish a bureaucratic United Nations Agency) is workable. Either puts business and the public at risk.

The "crime and nuisance" issues cannot be parked at the door of the law enforcement agencies. They have an important role but they will never have the resources or the expertise to cope with everything. Nor should they. Much of the nuisance and exploitation that outrages the public falls below the threshold for police action. In any event, crime prevention requires a comprehensive partnership approach and "authority to intervene" by police or the industry needs to be rooted in appropriate accountability and governance.

The "crime and nuisance" issues can be dealt with through the partnership approach proposed in this paper. The issues are separate but connected.

What's new about all this ?

Much of the criminal activity that exploits the Internet is already defined as criminal in the "real world" - what is new is the use of the Internet by crooks and their exploitation of new technology. The same happened with the development of the car and the plane and weaponry and publishing and modern retailing.

We know from such developments that no area of crime is dealt with by catching and punishing offenders alone. We also know that the public expect criminal activity to be prevented and dealt with – but they also expect accountability for the intervention of the authorities. Complex systems of accountability and governance have built up over centuries to manage those interventions – including national and international legislation, police authorities and the "crime reduction partnerships" that have reduced many aspects of crime and nuisance.

What is new is the speed and scale of the Internet, its global reach, the potential for multiple strikes and the vulnerability of the targets – from governments and international corporations to communities and individuals.

The temptation is for those who have the resources to build their defences and harden the targets – the same human responses that characterised both the Wild West and the Mediaeval period because governance was not comprehensive.

In the modern era, such an approach is unacceptable as well as ineffective. Some countries therefore want international "ownership of the internet" through a UN Agency – a concept that threatens the essence of the Internet.

This paper responds to the challenge of proposing a better alternative.

Unfortunately, issues of security are often separated from enterprise and development. People who are pushing the boundaries to develop new businesses or forms of communication are in the lead and those responsible for security are lower down in the pecking order of business – and of Government Departments.

That is changing - many businesses now see security as an essential element of cutting edge design – so there is an opportunity to broker a new approach.

Because exploitation of the Internet – for individual communication and for business and enterprise – requires maximum flexibility, a new approach is urgently needed, to link governance and accountability to a comprehensive partnership approach to analysing and preventing internet crime and nuisance.

Current fears and the existing environment

The proposals in this paper fully recognise the complex reality "on the ground".

Every conference on "cybercrime" hears horror stories of huge losses and we know that there have been some serious attacks on the infrastructure of business and government. But the evidence suggests that the costs of crime are relatively trivial as a percentage of on-line transactions or turnover.

They are of the same order as retail crime, for instance, where a certain level of "shrinkage" is accepted as the inevitable price for making your goods attractive and easily accessible to potential customers.

But the nature of the Internet – and the growth of organised crime rather than "attacks by geeks" – means that **potential** threats are big, real and immediate.

Public fears are compounded by the fragmentation and duplication of reporting and intelligence systems and by studies that mix the cost of attacks on the infrastructure with that of old crime exploiting a new medium. That doesn't help the development of a strategic partnership approach - but it also makes it difficult to make business cases for serious investment in crime prevention programmes - See Annex 1 for a summary of current UK and International systems see Annex 2 for a summary of relevant initiatives.

Individuals, businesses and public bodies all share responsibility for their own protection. But they need clarity about the environment in which they live and work - and the current situation is difficult for even the expert to navigate with confidence. The devil is in the detail of defining and improving the self-protection skills of users (from children and consumers through call centre and administrative staff to risk managers), the security skills of suppliers (from retail support staff through consultants to product designers and researchers) or the e-skills of investigators - see Annex 3 for a summary of relevant accreditation mechanisms, courses and qualifications.

Most successful crime reduction programmes include co-operation between business and law enforcement to reduce temptations and opportunity by redesigning the environment (e.g. shopping mall or housing estate) as well as engagement of the customers (the public). The tensions within the ICT community over who should do what with regard to "designing out" on-line temptations and opportunities are summarised in Annex 4.

Meanwhile on-line crime crosses all known policing, regulatory and jurisdictional boundaries and most enforcement involves partnerships in which the private sector contributes most of the resource – see Annex 5 for summary. This raises issues of governance of on-line policing and of the Internet itself. History shows that when governance issues are ignored in order to deal with an immediate threat, corruption often follows and law enforcement is compromised.

That is why it is so important to note that Governance of the Internet was central to the World Summit on the Information Society in Tunis in 2005.

Last week, the UK's consultation workshop on issues to be raised at the Internet Governance Forum in Rio de Janeiro in November found that security was by far the most important intra-UK issue, albeit ranking more equally with access and openness as issues at the International level.

Issues of threats to the infrastructure, serious crime and multiple attacks or scams are part of the total environment and cannot be separated from issues of business exploitation and personal safety. Safety online cannot be dealt merely as a security issue. It is linked to the need for coherent Internet Governance.

Again, off-line lessons can be applied. Local police work and crime prevention work take place in a framework of statute, common law and public administration (accountability) that has built up over centuries. Crime prevention requires a strong partnership – it cannot be left to the police alone. National police work takes place within that framework, as does the international dimension.

The same must apply online – but we do not have the luxury of time. We need a new style of governance linked to a new way of tacking crime and abuse on the internet if we are to both be effective and avoid the problems of international bureaucracy and top-down regulation.

Proposing a UK approach to governance and safety

Internationally, views are polarised between those countries that want to "leave things as they are" (in order to make sure that this fast-changing environment of communication and business is not constrained by bureaucracy) and those who want governance through an international structure or UN agency.

The Internet Governance Forum – a UK proposal – has provided a "space for dialogue" and avoided the risks inherent in either extreme. But agreement is fragile – the IGF must develop quickly or demands for "an Agency" will grow.

Instead of providing theoretical alternatives, the UK is now well placed to pave the way by creating the UK Internet Governance Forum (the UK IGF) as agreed last week. This also provides the opportunity to create the UK Internet Crime Reduction Partnership and to develop an industry-led UK Internet and ICT Complaints Centre. This will protect confidence in the Internet for business and the citizen. Replacing the "governance of the Wild West" with "governance through partnership" will be both modern and flexible.

SUMMARY OF THE PROPOSAL :

1. **The first issue is governance**. Nobody "owns" the issue of how the Internet should be regulated, but on the international stage the "British solution" – the IGF - avoids both the danger of piecemeal regulation by vested interests and the bureaucratic option of a new UN Agency.
2. The so-called "freedom of the internet" is already constrained in many ways – by commercial operators, Internet Service Providers and nations (China - free speech, USA - off-shore on-line gambling, UK - child abuse).
3. We can ………….
    - (a) leave it to companies and countries, the "Wild West option"
    - (b) go for "international ownership" through a bureaucratic "UN Agency" approach, or
    - (c) develop a Third Way solution – a partnership approach - which this paper advocates.
4. **The second issue is crime**. Criminals are bound to exploit the internet and ICT generally, but we need to end the mythology about "e-crime". It is not out of proportion to other crime, but the speed and capacity for "multiple strikes" mean that a new approach is needed. Police resources will always be

limited – so we need a non-Governmental approach to crime reduction to complement and co-ordinate the work of the police and the many self-protection and security operations of industry.

5. The proposals are designed to tackle both of these problems, have been tested with a variety of experts within Government, Industry and "Civil Society" (Third Sector) and have the endorsement of the Government. There is general agreement that we need to pull together Governmental and Non-Governmental approaches. This would not work as a traditional "Government initiative" but the proposals can be implemented quite quickly - provided the main players "sign up" to industry leadership.

6. The starting point on Governance is to show how the Internet Governance Forum (IGF) can be a better option than a UN Agency by "walking the talk", creating a UK IGF, owned jointly by Industry, Government, Parliament and "Civil Society". That was endorsed during the consultation meeting last week.

7. The starting point for tackling crime is for the same 4-way combination to be involved in the creation and governance of an Industry-led initiative for a UK Internet and ICT Complaints Centre, taking information on abuses and complaints from members of the public, public bodies, industry etc – so that Industry can "design out" the whole range of "crime and disorder" on the internet etc, down to the "e-graffiti" which affects everyone. Essentially it will be the UK's "crime reduction partnership" for ICT and the Internet.

8. This will **complement** the proposed police (Met/ACPO) unit – which is an essential development - and be designed in collaboration with them so that "intelligence" is passed up quickly. It will also complement the Fraud Reporting Centre currently being designed by ACPO and the City of London. And it presumes the continued development of specific initiatives such as the National Information Assurance strategy, led by the Cabinet Office, and a variety of initiatives on information exchange, internet security etc. It provides answers to the questions posed by the excellent report published this summer by the House of Lords Select Committee.

On both the "Governance" issue and on "e-Crime" I conclude that ……

a. There are real problems, not owned anywhere within Government, although several Departments (DTI – now Department for Business - Home Office, Cabinet Office, the Attorney General etc) are increasingly concerned and separately engaged with industry.

b. The issues do not respect national borders, but the UK is uniquely placed to take a new "partnership approach" which can influence the international community approach and boost our reputation as the best place to do international business.

c. Industry is increasingly willing to sign up to a partnership approach (and through our approach to child abuse has learned the value of partnership as a real alternative to regulation).

d. A coherent police approach is being developed through the proposed Met/ACPO e-crime unit.

e. We will be effective only if we connect governance and accountability – both live issues internationally – to crime reduction.

These ideas were first explored with a variety of players on a confidential basis, including the UN's IGF executive co-ordinator, representatives of the Met/ACPO, a variety of Industry players, including some major companies, as well as Nominet, Intellect and the CBI, and also with the then Prime Minister and with the Ministers and Officials most directly involved with the two issues in the relevant Departments. On behalf of the Government the Home Secretary has supported this approach as has the lead Minister, Rt Hon Stephen Timms MP at the Department for Business.

None of this conflicts with the detailed work taking place across Government departments or the initiatives within the Industry, or the Met/ACPO initiative but it provides the effective framework of accountability that is essential in a democratic society. We will now build up a genuine partnership model with the support of all parties and industry buy-in and outline this approach at the IGF in Rio where the UK can show a "team presence" of the partners. In parallel we need to work on the European and International dimension.

The intention is to work speedily on the development of partnership through both the "UK IGF" and the UK Internet and ICT Complaints Centre in order to have both in place by the middle of next year and provide evidence from the "working model" for the 2008 Internet Governance Forum. Such a timetable is ambitious, but not impossible.

The consultation workshop on 18th October provides the opportunity to seek wider agreement. Please can I have your united support in taking this forward – and also your comments and suggestions on how to do so?

Yours sincerely,

Alun Michael

PARLIAMENT AND THE INTERNET
CONFERENCE - 18 October 2007

THE EUROPEAN
INFORMATION
SOCIETY GROUP EURIM

ANNEX 1

Reporting and Intelligence: How do we know what is happening?

1 Summary: A fog of fragmented systems competing for attention

Most so-called cyber-crime is traditional crime using a new medium. Extortion backed by a denial of service attack is old-fashioned extortion and a “death threat” is a “death threat”, whether it is through the letterbox, over the phone or by e-mail. Many organisations compete for budgets to monitor what is happening and for the time of knowledgeable victims to report on their experiences. Their terms of reference, resources and competence vary. The priorities they address include: threats to critical infrastructures, including the Internet itself; helping large organisations protect themselves and their most important customers; supporting the sale of security products and services to business and consumers; helping law enforcement respond to criminal activities which fit their key performance indicators; helping mass-market service providers protect paying consumers; helping different types of law enforcement, information assurance, electronic and communications security and investigation professionals and suppliers address their segmented objectives. The consequent differences of approach and of definition help explain why the recent House of Lords enquiry found so much confusion over the scale and nature of the threats to Personal Internet Safety.

Has the on-line world become part of the mainstream of human life? Are consumers no more vulnerable at home to cyber-mugging (ID theft and fraud) than to being mugged in the street outside and children no more vulnerable to cyberbullying in their bedrooms than to playground bullying? If so, is the task to educate children, their parents and their grandparents to go safely on-line to buy, sell, save, learn and play? Or are most problems caused by a few dozen global criminal syndicates harnessing a couple of hundred spammers and their botnet armies? If so, would it be more cost-effective to put a fraction of the billions currently spent on information and communications security into international co-operation to track, trace and remove them?

2 Critical Infrastructure Reporting and Response Teams

There are over 250 “Computer Emergency Response Teams” (CERTs) worldwide, linking into a highly automated global incident, reporting, tracking and response operation, funded jointly by industry, FBI and the US and hosted in Pittsburgh by the National Cyber Forensic Training Alliance (NCTFA). Many of the global infrastructure, applications and communications service suppliers, financial services and e-commerce suppliers, defence/aerospace and pharmaceuticals multinationals have global incident response teams which link direct to the NCFTA. The main UK public sector CERT, Unified Incident Reporting and Alert Scheme (UNIRAS), is part of the Centre for the Protection of National Infrastructure (CPNI) which interfaces with the Police National Counter Terrorism Security Office (NaCTSO) and a network of geographic and sector “Warning Access and Reporting Points” (WARPS).

3 Alert Services for large organisations

Many commercial services monitor on-line products and services. Analyses and reports provided by organisations such as BT Counterpane, Symantec, Mark Monitor and Secunia enable vendors of anti-virus software, spam filters and other protection tools to update their products and services and to warn subscribers of vulnerabilities or pending attacks so they can take appropriate action.

4 Alert services for small firms, consumers and parents

IT Safe warns about recently discovered vulnerabilities. The National E-Crime Prevention Centre plans to support WARPS for local government, healthcare and small firms in the East and West Midlands and also schools, rural businesses, business and science parks and biotech industries. The Metropolitan Police Fraudalert reports the changing patterns of fraud. The Child Exploitation and On-

Line Protection Centre runs an integrated service covering advice, guidance and reporting. The Internet Watch Foundation runs a hotline for reporting potentially illegal child sexual abuse content and a 'notice and takedown' service to any British service provider hosting such material.

5 Crime Reporting and Intelligence Services

US victims of cyber-crime have a convenient and easy-to-use reporting mechanism via The Internet Crime Complaint Centre (IC3) for suspected criminal or civil violations and through the US Federal Trade Commission for ID Theft. The UK has no equivalents. Current advice is to report to a police station, anonymously via Crimestoppers, or via a non-emergency notification website (which is currently unavailable, pending the testing of a new system). The Fraud Alert website suggests that phishing e-mails be sent to Bank Safe Online or direct to Paypal or eBay as appropriate.

APACS, the UK payments association, runs a "Fraud Intelligence Bureau" based on reports from its members and an "Industry Hot Card File" of lost or stolen cards. There are plans to merge these with the intelligence function of the "Dedicated Cheque and Plastic Card Unit" to form a "Payment Industry and Police Joint Intelligence Unit". A "Fraud Intelligence Security System" is under development to enable intelligence sharing between UK retail banking and card institutions, the Serious and Organised Crime Authority, the Metropolitan Police Service and the new National Fraud Reporting Centre. This will include inputs from the "Credit Industry Fraud Avoidance Service", which maintains lists of known or suspected fraudsters so that their subsequent attempts to defraud its members can be more rapidly identified.

The Serious and Organised Crime Agency does not provide a reporting service except for money laundering and terrorist funding. It became responsible for these after the Review of the Suspicious Activity Reporting Regime found "a perception in the regulated sectors that the SARS regime is broken: that institutions are spending some millions of pounds complying with burdensome legal regulations, yet Government is not similarly committed and there are virtually no results …."

Experian, Equifax and others run a variety of reporting and intelligence operations on behalf of financial services and insurance companies. The main communications and managed service providers also run internal reporting and intelligence services, some of which, where allowed, exchange information with police and government services around the world. The providers of international alert and anti-malware products and services also have processes for monitoring traffic, collating reports from customers and exchanging threat information with each other.

Most UK communications service providers have routines for their customers to report malpractice and "Bank Safe On-line" runs a collective service for those who receive "suspect" e-mails from "their bank". Reports are, however, rarely acknowledged. There is therefore a proposal for an e-victims service to help users identify what has happened and advise what (if any) reporting elsewhere should be done. The service will help its promoters to provide better support at lower cost but it is best viewed as a "first stop shop" to filter out experiences that are not individually reportable.

6 Attempts to Bring the Scene Together

There have been a number of attempts to assess the scale and cost of e-crime in the UK, using a variety of definitions. Market research in 2006 showed that consumers felt more likely to be victims of e-crime than of car crime, burglary or mugging, and there is a risk that this will undermine confidence over time although at present other surveys indicate that annoyance or even losses at present levels are seen by many as an acceptably low price to pay for convenience.

There are many proposals for new reporting and intelligence services, including at European level, but the prime need appears to be to combine a single doorway for communicating concern and complaints linked to improving the efficiency of current services in ways that will help target effective action and to the ACPO/Met "Police Central E-Crime Unit", (see diagram in Annex 5. It is important that people are clear that the police unit will not be able to deal with every incident notified to the proposed complaints centre, which is why the two proposals are separate but connected. Both services will need clear links to the US IC3 reporting centre and the NCFTA "reaction" centre in Pittsburgh. Governance is crucial to ensure that sensitivities about protection of data, management of confidential reports and commercial sensitivities are properly protected.

PARLIAMENT AND THE INTERNET
CONFERENCE - 18 October 2007

ANNEX 2

THE EUROPEAN
INFORMATION
SOCIETY GROUP EURIM

On-Line Crime Prevention Programmes

1 Summary: much awareness, some guidance, the beginnings of action

Until recently most on-line service providers were focussed on providing low cost, user-friendly access. E-crime prevention was seen as little more than encouraging users to buy and use anti-virus filters and firewalls. Law enforcement and government therefore gave it a similarly low priority. Financial services have given it rather higher priority, but are focussed on preventing costs and losses to themselves and their customers. And most e-crime by reported value, if not by volume, harm or distress, involves insiders, including those who copy files of customer, client, patient or supplier details and/or help bypass security controls.

Crime prevention programmes tend to have five main threads:

- promoting awareness of the risks and need to take action;
- support programmes, including to install and inspect/maintain security products and services;
- advice on risk management/avoidance, given the need to live/work/play in a given specific environment;
- education and training: from personal risk avoidance through crime prevention and security staff to those in a position to "design out" product, service and environmental vulnerabilities;
- risk reduction. to re-engineer the environment to make criminal behaviour less attractive.

All of these have the potential to make a significant contribution to the proposed "Crime Reduction Partnership" and Complaints Centre which will aim to broker a joined-up UK approach to on-line crime and nuisance.

2 Awareness

"Get Safe Online" is the nearest the UK has to "a comprehensive unified source of information on online safety and security" (House of Lords Report). It is sponsored jointly by Cabinet Office, DBERR, Home Office, CPNI, Cable & Wireless, eBay, HSBC, Microsoft, SOCA and Symantec. It links to other sites, including "IT Safe" for alerts on vulnerabilities, "Bank Safe Online", "Card Watch" and a Home Office website on identity theft. There are similar programmes in the US, "Stay Safe On-Line" and at EU level, "Be Safe On Line". Most awareness sites also provide crime prevention advice: e.g. The "Personal Security Plan" or the "Spot and Stop Card Fraud retailer training pack", available for download from the Card Watch site..

Childnet International has a remit to make the Internet "a great and safe place for children". It works with DCSF. (with which it has recently published guidance for schools on preventing and responding to cyberbullying), and the Child Exploitation and On-Line Protection Centre, which has integrated services covering advice, guidance and reporting. The Internet Watch Foundation runs a hotline for reporting potentially illegal child sexual abuse content wherever it originates and a 'notice and takedown' service to any British based provider hosting such content.

3 Support for consumers and small firms

Most e-crime prevention advice refers to fitting anti-virus protection and firewalls as being the electronic equivalent of fitting locks and alarms. However, the UK National Security Inspectorate does not cover electronic security systems (other than fire and burglar alarms etc.) and the professional bodies and trade associations for the ICT industries were united in their opposition to the Security Industry Authority covering those providing electronic security advice, guidance and support. The House of Lords found much difficulty in understanding what current products and services do or do not do and called for the proposals for a BSI kitemark for content filtering (supported by the Home Office and Ofcom) for child protection purposes to be extended to cover security software. ID theft is a major

concern and Experian, Equifax and Garlik offer chargeable services to alert consumers when anyone seeks to take out credit in their name.
The Metropolitan Police Service has delivered e-crime awareness training to its 140 Crime Prevention Officers with a view to the messages being delivered to individuals and SME's across London and maintains the Fraud Alert website which offers e-crime awareness advice to individuals and business.

Yorkshire Forward and its four regional police forces run a web portal to enable ICT adopters in SMEs to check their e-security vulnerabilities and undertake some basic training. It also funds a business crime reduction centre which supports field officers co-located with the local Chambers of Commerce.

Advantage West Midlands, West Midland Police and the Cybersecurity Knowledge Transfer Network support a "National E-Crime Prevention Centre" which will be a hub for research and training and host crime prevention support services for small firms, local government and healthcare.

The national register for Warning, Advice and Reporting Points lists four public sector WARPs (e.g IG WARP for the National Health Service), seven for local government (e.g. SKWARP for Local Authority Partners in Kent), two for business, two for the voluntary sector and one international.

4 Support to Schools and Colleges

The British Educational Communications and Technology Agency has a remit to provide advice and guidance to schools when they request it. The Regional Broadband Consortia organise on-line services for schools and most require suppliers to provide guidance to the schools they serve, whether requested or not. UKERNA runs the UK's Joint Academic Network and its security team provides advice and guidance to those connected to the network.

5 Support to large organisations

There is a billion pound industry selling "security solutions" to those who can afford to pay for customised services with a variety of professional bodies, trade associations and security "clubs".

TUFF (the Telecoms UK Fraud Forum) and MICAF (the Mobile Industry Crime Action Forum) share offices, staff, best practice and training across the main communications suppliers.

CIFAS (the Credit Industry Fraud Avoidance Service) maintains lists of known or suspected fraudsters so that their subsequent attempts to defraud its members can be more rapidly identified). The APACS Industry Hot Card File (IHCF) enables retailers to check transactions against lost or stolen cards.

The Jericho Forum brings together many of the world's largest users of security products and services to "define ways to deliver effective IT security solutions that will match the increasing business demands for secureIT operations in our open, Internet-driven, globally networked world".

The "National Information Assurance Strategy for the UK" is owned by "The Officials Committee on Security" (Chief Information Security Officers), the "Information Assurance Policy and Programme Board" and the CIO Council and driven by CSIA, CESG and CPNI and their industry groups.

6 Advice on Risk Management

Advice on avoiding unnecessary risks and recognising potentially dangerous situations is a common thread in mainstream crime prevention programmes but is at odds with the business models of many players. Thus evidence to the House Of Lords highlighted the clash between advice not to give out personal information and the regular encouragement to give this out on social networking sites. There is also a need for greater awareness among those wishing to deal with their customers/clients/voters on-line as to what is good practice with regard to safeguarding customer information. Recent fines imposed by the Financial Services Authority, the Information Commissioner's proposed Code of Practice and the latest Californian legislation concerning information that could be used to aid fraud may all help stimulate this.

7 Education and Training – see Annex 3: Defining and Delivering e-Security and Investigation skills

8 Risk Reduction – see Annex 4: Designing out E-Crime: Removing vulnerabilities and reducing temptation

PARLIAMENT AND THE INTERNET
CONFERENCE - 18 October 2007

THE EUROPEAN INFORMATION SOCIETY GROUP EURIM

ANNEX 3

Defining and Delivering e-Security and Investigation Skills:

1 Summary: No-one has policy responsibility for on-line self-protection or security skills

The House of Lords report on Personal Internet Safety found that “Government’s well-intentioned efforts to raise awareness of e-crime, without paying enough attention to the ways in which individuals or businesses can protect themselves against it, are actually making the problem worse”. It called for the Department for Children, Schools and Families to find new ways of educating adults, as well as children, in online security and safety. Its other recommendations require much action on the skills of industry and law enforcement.

Skills requirements are commonly defined as rungs on ladders. Thus the bottom rung on the “personal e-protection ladder” might be: “basic security awareness, the ability to use pre-installed mass-market security facilities and to know where to go for help”. Higher rungs on the ladder for those running corporate systems might include “to ensure that existing products and services are configured securely” or “that new products and services do not contain unnecessary vulnerabilities”. Most on-line crime is, however, old crime exploiting new and evolving media. Therefore the “rungs” and “ladders“ can change shape and direction at short notice. They are akin to the staircases in The Hogwart’s School of Witchcraft and Wizardry rather than the traditional career paths assumed by UK education and training structures.

The UK hierarchy for defining educational and occupational standards and accrediting the qualifications leading to them, (the Quality Assurance Agency, the Qualifications and Curriculum Authority, the Sector Skills Councils etc.) does not cover self-protection, crime prevention, security and investigation skills in the detail necessary to plan course provision or career development. This role is spread over a variety of organisations, united mainly in their opposition to that role being taken by the Security Industry Authority.

The skills needed are, however, international and most widely recognised qualifications are accredited via ANSI (American National Standards Institute) rather than UKAS (UK Accreditation Service) although the UK developed “Skills Frameworks for the Information Age” (SFIA) is used by many large employers internationally to plan staff training and development. SFIA includes definitions for Security Administration and for Information Security as a whole, at levels 3 (technician) to 6 (setting corporate policy).

2 Personal Internet Safety and End User Skills

There are many ICT end-user qualifications but the only one known to cover on-line safety, self-protection and good citizenship is the Scouting Association Award, supported by BCS and now held by over 40,000 scouts and guides. The “Spot and Stop Card Fraud” education pack and training programme, developed by the banks in collaboration with retailers, police and organisations like Crimestoppers, is probably the largest single UK fraud prevention training programme to date. APACS, the UK payments association, the British Bankers Association and CIFAS, with Home Office backing, have also produced online training for businesses that could be targeted by identity fraudsters. Many large organisations, especially in the financial services, provide mandatory training on basic systems security, including data protection, to all staff. Some make their programmes and material available to the families of staff - but there are no known shared certifications, nor any plans for them.

3 Professional and Technical Skills

The main commercial ICT training providers, University short course operations and several dozen security consultancies offer training leading to the qualifications in most demand (e.g. those to configure the security features of Microsoft and CISCO products). In aggregate, these cover a wide range of skills - from how to use the security facilities already built into mainstream operations, through the use of specific forensic analysis tools to non-certificated courses on investigating crime which makes use of e-Bay transactions.

The "generic" (i.e. non-product specific) certifications, most likely to be required by employers and most valued by professionals are those from:

ISC2: International Information Systems Security Certification Consortium (over 50,000 individuals certified in 129 countries, including more than 2,300 in the UK). These include: SSCP (Systems Security Certified Practitioner) and CISSP (Certified Information Systems Security Professional).

ISACA: Information Systems Audit and Control and Control Association: including CISM (Certified Information Security Manager) and CISA (Certified Information Security Auditor).

ISEB: Information Systems Examinations Board (part of the British Computer Society): CISMP (Certificate in Information Security Management Principles) and CIRM - Certificate in Information Risk Management).

GIAC: Global Information Assurance Certification: for the United States National Security Agency and other US government agencies and private sector bodies. This appears to be valued much more widely than its UK equivalent, **ITPC** (Infosec Training Paths and Competencies), although the latter is supposedly mandatory for those working on secure systems for HMG.

At the technician level the most widely recognised qualification appears to be "security +" produced by COMPTIA, the US-based Computing Technology Industry Association, set up in 1983 to improve the skills of dealer support staff and now supported by almost all the main US suppliers

There are many special interest groups and registers ranging from those of the BCS for "information systems security" and "information risk management", through the Information Assurance Advisory Council to trade associations and practitioner groups like: the Alliance Against Counterfeiting and Piracy, the High Technology Investigators Association, the Information Security Forum, the Internet Enforcement Group, the Mobile Industry Campaign Against Fraud, the Risk and Security Management Forum, the Security Professionals User Group and the Telecommunications UK Fraud Forum.

The Institute for Information Security Professionals (**IISP**) was created to avoid pressure for electronic security professionals to come within the remit of the Security Industry Authority and has over a thousand associate members and support from around 30 large employers (both public and private sector). Its active membership overlaps with that of the UK chapter of the Information Systems Security Association (**ISSA**) which has around 14,000 members world-wide, 1,100 in the UK and brings together those accredited by others for mutual education and action programmes (e.g. e-crime awareness and prevention).

4 Law Enforcement Skills

The National Policing Improvement Agency runs a "First Responder" course, a Masters in Cybercrime Forensics and some more specialist courses. Several forces use local Universities to provide similar programmes or have packaged and on-line material available in their training centres.

5 Educational, Academic, Research and Development Skills

Information security and on-line safety are due to be included in the next revision of Key Stage 4 in schools. They are not mandatory in most UK undergraduate computer science or business IT courses but students are commonly offered basic security training when they sign up to the computer network of their university. There are also at least five current or planned undergraduate degrees in ICT Security (various titles) and/or Forensic Computing. There is also a growing number of post graduate and mature entry courses covering varying mixes of information security and forensics. A recent survey showed that both professionals and employers place a high value on the MSc and MBA programmes of Universities such as Cranfield, De Montfort, East London, Glamorgan, Royal Holloway, Portsmouth and Westminster. The research director of a multinational which bases its global Information Security R&D in the UK has said, however, that most of their best graduate researchers now come from outside the UK education system.

PARLIAMENT AND THE INTERNET
CONFERENCE - 18 October 2007

ANNEX 4

THE EUROPEAN
INFORMATION
SOCIETY GROUP
EURIM

Designing Out E-Crime: Removing vulnerabilities and reducing temptations

1 Summary: applying crime reduction principles to on-line malpractice requires choices

The House of Lords report on Personal Internet Safety called for a review of responsibilities and liabilities to encourage those wishing their customers go on-line to do more to help protect them, including by working together to improve the security of products and services. Nearly five years ago the DTI-supported Foresight Programme into Cyberbersecurity similarly identified a need to apply "crime science" principles to the criminogenic (i.e. attractive to criminals) features of information systems, the Internet and E-commerce.

The "Internet" has no "security" layer but there has been much work on the use of encryption technologies to "authenticate" traffic and enable secure communications between those willing to pay extra. Their deployment, however, entails many trade-offs and what is "practical" is a matter of business models, intellectual property rights and cultural values, as much as of software engineering. Thus, security features common to most of the servers and routers that underpin the Internet are often switched off by those providing fast response or low cost services to researchers (who need raw power/speed) or consumers (who want fast response multi-media).

The House of Lords concluded: "well-targeted incentives are more likely to yield results in such a dynamic industry than formal regulation". They recommended, for example, giving Banks responsibility for securing on-line transactions akin to those they have for those off-line, under the Bills of Exchange Act 1882. There are also calls for Internet Service Providers to take greater responsibility for the material they carry or host. But the Law Commission commented in 2002 that "notice and take-down" regimes give ISPs no incentive to check the validity of complaints.

Meanwhile, there appear to be stronger economic incentives for software and service suppliers to compete in the provision of security add-ons than to co-operate in removing systemic vulnerabilities or disrupting the global malware supply chain (automated spam and increasingly sophisticated phishing tools to deploy worms, viruses, Trojans and assorted spyware etc.) The result is an expensive arms race. In the name of "e-crime prevention", consumers and small firms are encouraged to install software to filter out known or suspected malware, or block attempts to visit websites which may carry illegal/undesirable content or to support criminal activity.

There is also a tension between those who wish to see the systems and services of large organisations (e.g. banks and government) made more resistant to misuse by staff, contractors or customers and those who see current losses as an acceptable cost of doing business. Even basic principles such as:

- security should be easier for the user than insecurity;.
- security should be cheaper for the user than insecurity;.
- security should be a community issue;.

do not have universal acceptance within the Internet communities - which are focussed on ease of use and facilities, with security as an add-on cost, both time and money: "no gain without pain".

2 Improved information

There appears to be potential agreement on the provision of:

- easier ways for users to establish how secure their systems are, the threats they face and the balance of risk, facilities, ease-of-use and speed appropriate to their applications: leisure, learning, business etc..
- schemes that indicate clearly what security facilities are built into which products and services and the security profiles/standards to which they conform: from basic consumer information packs through to more detailed information for technicians and professionals;

- pre-installed security facilities, configured to the security levels required by the average user, with clear information on what this means and how to change the balance of facilities, performance and security.

3 Filtering versus Authentication

Large scale monitoring and filtering, while profitable to suppliers could be more destabilising than the wider use of existing traffic authentication technologies. It is, however, one thing to provide authentication services for organisations willing to sign up to the protocols of IdenTrust (for transactions underwritten by banks), secure transaction services like those provided by VocaLink (for business payments) or those proposed by TWIST (for supply chain transactions): all of which are underpinned by contractual acceptance of liability as well as responsibility. It is something very different to try to provide such services to those claiming crown immunity or consumer protection rights to avoid responsibility, whether for their own actions or for that which is genuinely outside their control. Moreover, the secure transmissions of business produce many fewer packets of data than those of consumers.

4 Current Filtering Initiatives

There are many automatic filtering systems which will remove traffic to or from blacklisted sources, containing key words or patterns, or according to content ratings. Other services involve active monitoring by panels of volunteers or contractors looking for breach of copyright or court order, or that of which local governments or content regulators do not approve. It is said that filtering is best done before traffic enters the “Internet”. That would require co-operation between independent players operating under different jurisdictions around the world and could well lead to a polarisation of services that is vigorously opposed by major players in the name of “net neutrality”.

5 Current Authentication Initiatives

“Chip and PIN” is credited with halving face-to-face card fraud in the UK over the past two years, but this reduction has been balanced by a rise in card-not-present fraud. Secure payment systems recently introduced by Visa and Mastercard allow cardholders to register an additional password for use when shopping online at participating retailers. In a similar effort to reduce on-line banking fraud, customers are now being issued hand-held card-readers, which generate a one time number when the user’s card is inserted. This combined with their PIN number provides two factor authentication.

6 National and International Trust and Identity Management Services

There are many ID management schemes competing to provide “answers” to the problems of on-line impersonation. Some of these are linked to the extension of the residents’ registers and associated low security “ID cards” that are common to central and local government around the world. Others are linked to national security concerns, frequent flier programmes or the facilitation of authenticated on-line transactions. Some governments, as in the UK, aspire to link these together in common frameworks.

The trust and transaction systems of the financial services industries embrace those willing and able to accept contractual responsibility for their actions. IdenTrust (created to enable cross-border electronic commerce) and SWIFT (created to service correspondence banking), now enjoy symbiotic relationships with each other and with organisations like VocaLink, which handles payment clearing, including the high street cash terminals. In parallel we have alliances of technology suppliers, like the Liberty Alliance, to provide interoperable “federated” identity standards at product/service level.

7 Information Assurance Initiatives

The “National Information Assurance Strategy for the UK” is owned by “The Officials Committee on Security” (Chief Information Security Officers), the “Information Assurance Policy and Programme Board” and the CIO Council. It will be driven forward by the Cabinet Office. CSIA, CESG and CPNI with industry collaboration via groups such as the Crypto Developments Forum and the Information Assurance Collaboration Group. The Information Commissioner has consulted on a Code of Conduct and there are plans for a cross-government Identity Management Standards Group.

PARLIAMENT AND THE INTERNET CONFERENCE - 18 October 2007

ANNEX 5

THE EUROPEAN INFORMATION SOCIETY GROUP EURIM

Cyber-Crime Investigation and Enforcement

1 Summary: most investigation and enforcement is by the private sector

A study in January 2005 found that “The total funding available to the NHTCU [National High Tech Crime Unit] (including for supporting computer crime units) is less than the individual electronic security and investigation budgets of most major High Street banks or of the main network or outsource suppliers”. In April 2006, most of the staff of the NHTCU moved across to the E-Crime Unit of the Serious and Organised Crime Agency (SOCA) which has more than twice the resource but a narrower remit.

The House of Lords enquiry “heard considerable scepticism over the capacity of the police and criminal justice system in this country to enforce the law.” They felt it essential to correct the perception that “the police do not seem to have anywhere near the capability to respond to these types of crime effectively”. They called for “Home Office, without delay, to provide the necessary funds to kick start the establishment of the Police Central eCrime unit, without waiting for the private sector to come forward with funding.” Until then, the policing of the on-line world, as with that of the railways in the 19th Century, is being conducted and funded almost entirely by industry, whether to protect its infrastructure from theft or terrorism or its customers from theft, fraud and impersonation, and is currently fragmented which is why a comprehensive partnership approach is urgently needed.

2 Law Enforcement and Regulatory Agencies, including joint units

The Metropolitan Police is the lead force on e-crime and its Economic and Specialist Command contains a computer crime unit (about a dozen officers) focussed on offences committed under the Computer Misuse Act: primarily hacking, denial of service and the creation of malware. Separate teams address ID theft and fraud and film piracy (in “partnership” with industry). The “Dedicated Cheque and Plastic Crime Unit” (DCPCU) is fully “sponsored” by the banking industry, including fraud investigators and administrators to work alongside police officers and civilian staff from the City of London and Metropolitan Police to tackle the organised criminal gangs responsible for the majority of cheque and plastic card crime in the UK. “Special Branch” has its own team (for monitoring the on-line activities of terrorist groups) as does the Child Abuse Investigation Command which works closely with the Child Exploitation and Online Protection Centre (CEOP). CEOP delivers “a holistic approach that combines police powers with the dedicated expertise of business sectors, government, specialist charities and other interested organisations – all focussed on tackling child abuse wherever and whenever it happens.”
.
The E-Crime section of the Serious and Organised Crime Authority (SOCA) has an establishment of about 80 staff and is primarily concerned with the use of the Internet by organised crime to aid drug and people trafficking, individual and private sector fraud and money laundering.

Over 300 agencies have investigatory powers under the Regulation of Investigatory Powers Act and previous legislation. Many, such as the Department of Work and Pensions, HM Revenue and Customs and Royal Mail, have their own investigation teams and prosecuting powers. Some have capability for investigating on-line crime. They include the Information Commissioner, who can take action in the event of breaches of the Data Protection Act, the Financial Services Authority, which can take action against those who do not have adequate protection in place, and ICSTIS, the premium rate services regulator, which has a remit to act when Internet scams involve the use of premium rate phone-lines.

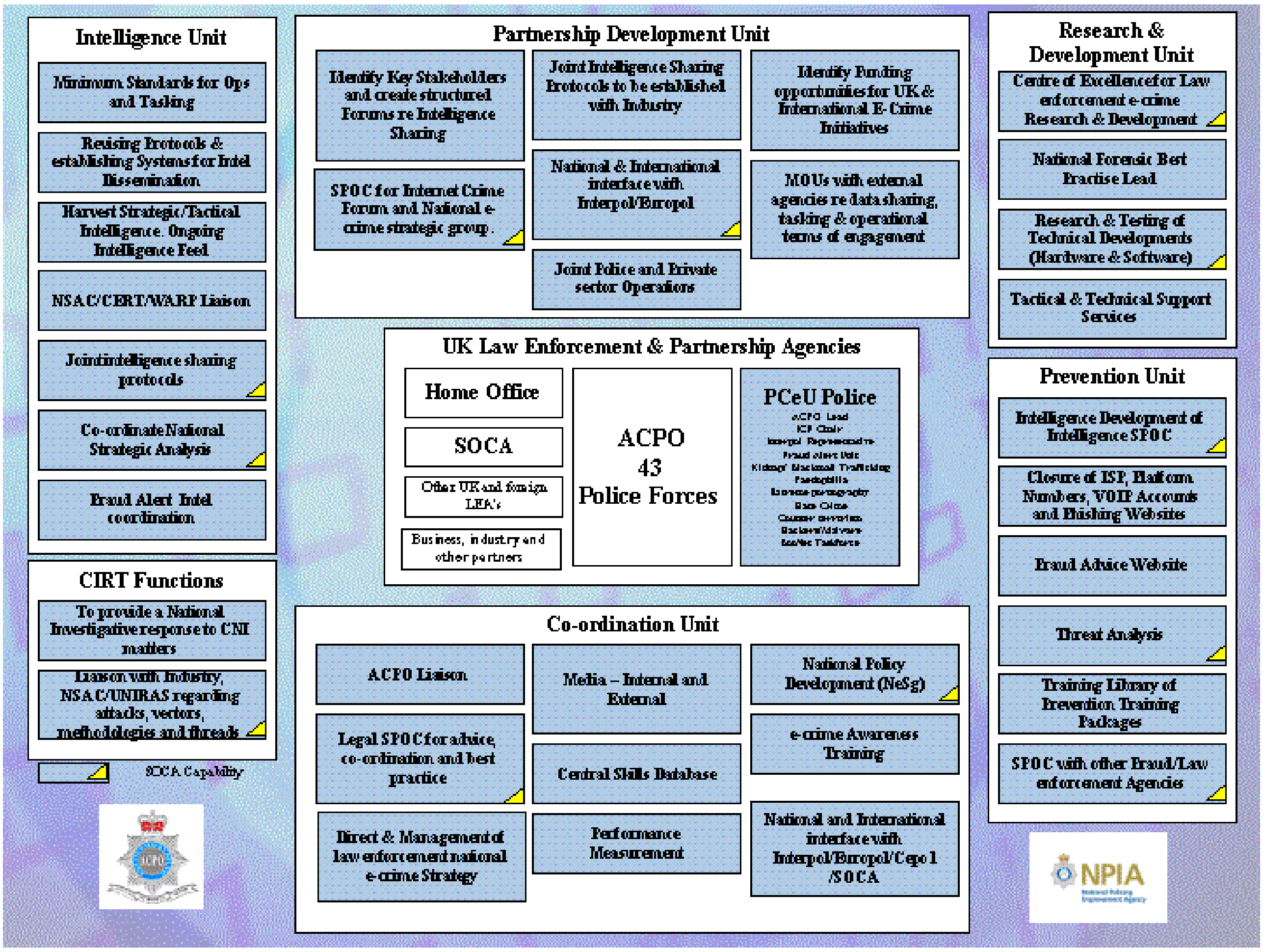
3 Industry Groups and Players

The Internet Enforcement Group is a cross industry body of Internet investigators representing the book publishing, music, games, software, merchandising and firm industries. Their members organise and fund almost all investigations into on-line piracy and intellectual property theft in the UK, whether leading to criminal prosecutions involving the police and/or trading standards officers or to civil action.

The main telecoms players support TUFF (the Telecoms UK Fraud Forum) and MICAF (the Mobile Industry Crime Action Forum) which share offices and staff. The main banks and financial services players support units like the DCPCU via APACS, the British Banking Association and the Finance and Leasing Association. Many also have in-house fraud investigation teams, some significantly larger than the DCPCU. The multi-nationals in industries such as pharmaceuticals, aerospace, oil and gas routinely employ organisations with forensics teams and international investigation and law enforcement liaison expertise: such as Control Risks, Deloitte, Detica, IBM, KPMG, Kroll, LogicaCMG, QinetiQ, Siemens Insight etc. Some major suppliers also undertake pro-bono investigations on behalf of small customers and/or end-users.

4 Current Initiatives - Specialist Units and Specialist Constables

CEOP draws on the expertise of industry players, (like Microsoft, which also provides sponsorship and technical support for the IWF). CEOP uses panels of vetted industry volunteers (e.g. over a hundred from CISCO alone) to support education programmes, including via Childnet International. The Metropolitan Police is building up a cadre of Special Constables with IT expertise and is exploring routines whereby ICT suppliers and users encourage their staff to volunteer: akin to those used to encourage employees of major retailers to help police shopping malls. Other forces are known to be looking at e-Community Support Officers and Volunteers to monitor chat rooms and act as witnesses. By far the most important police initiative, which would be complementary to the crime prevention partnership approach and linked to it, is that of ACPO and the Metropolitan Police for a Police Central E-Crime Unit, drawing on industry support and working closely with SOCA, the City of London Police and a new National Fraud Reporting Unit – see below
:


Intelligence Unit
Minimum Standards for Ops and Tasking
Revising Protocols & establishing Systems for Intel Dissemination
Harvest Strategic/Tactical Intelligence. Ongoing Intelligence Feed
NSAC/CERT/WARP Liaison
Joint intelligence sharing protocols
Co-ordinate National Strategic Analysis
Fraud Alert Intel coordination
CIRT Functions
To provide a National Investigative response to CNI matters
Liaison with Industry, NSAC/UNIRAS regarding attacks, vectors, methodologies and threats
SOCA Capability
Partnership Development Unit
Identify Key Stakeholders and create structured Forums re Intelligence Sharing
SPOC for Internet Crime Forum and National e-crime strategic group.
Joint Intelligence Sharing Protocols to be established with Industry
National & International interface with Interpol/Europol
Joint Police and Private sector Operations
Identify Funding opportunities for UK & International E-Crime Initiatives
MOUs with external agencies re data sharing, tasking & operational terms of engagement
UK Law Enforcement & Partnership Agencies
Home Office
SOCA
Other UK and foreign LEA's
Business, industry and other partners
ACPO
43
Police Forces
PCeU Police
ACPO Lead
ICF Chair
Interpol Representative
Fraud Alert Unit
Kidnap/ Blackmail Trafficking
Paedophilia
Extreme pornography
Race Crime
Counter terrorism
Hackers/Malware
Co-ordination Unit
ACPO Liaison
Legal SPOC for advice, co-ordination and best practice
Direct & Management of law enforcement national e-crime Strategy
Media – Internal and External
Central Skills Database
Performance Measurement
National Policy Development (NeSg)
e-crime Awareness Training
National and International interface with Interpol/Europol/Cepol /SOCA
Research & Development Unit
Centre of Excellence for Law enforcement e-crime Research & Development
National Forensic Best Practise Lead
Research & Testing of Technical Developments (Hardware & Software)
Tactical & Technical Support Services
Prevention Unit
Intelligence Development of Intelligence SPOC
Closure of ISP, Platform Numbers, VOIP Accounts and Phishing Websites
Fraud Advice Website
Threat Analysis
Training Library of Prevention Training Packages
SPOC with other Fraud/Law enforcement Agencies
NPIA