

**Report of The Parliament and Internet Conference - 18<sup>th</sup> October 2007**  
**Workshop on tackling crime and achieving confidence in the on-line world**

## **Summary**

There was strong support for developing a practical and comprehensive approach to tackling crime and nuisance in the on-line world. There are growing concerns about criminals turning to the Internet to commit old crimes and invent new ones. The impact is not out of proportion with offline forms of criminal activity but the potential is enormous in terms of speed, penetration and multiple attacks. The police response is important but will only deal with an appropriate range of offences and cannot deal with a lot of low-level nuisance that causes public concern. The UK is already working on a positive approach to governance – arguing for partnership between Government, Parliament, Industry and Civil Society through a United Kingdom Internet Governance Forum. It is proposed that the same four-part governance oversee an industry-led “complaints unit” to better target corrective action – an approach which would complement both the proposed Police Central Unit and the National Fraud Reporting Centre which is now being established.

## **Introductory contributions**

The Rt Hon Alun Michael JP MP stressed that it was assumed that participants had read the advance paper [www.eurim.org.uk/activities/ecrime/PIC07\\_AdvanceNote.pdf](http://www.eurim.org.uk/activities/ecrime/PIC07_AdvanceNote.pdf). The precise scale and nature of the problems was unclear, partly because of confusion over definitions as well as measurement. But it was far bigger than the police would be able to handle with the resources ever likely to be available to them in even the most optimistic scenario and required international co-operation. A top-down “United Nations” agency bureaucratic approach would not work. “Leaving it to industry” was equally unacceptable because it could perpetuate the current chaos and properly raise issues of accountability. Partnership through some form of e-Crime Reduction Partnership was essential – reflecting legislation, governance and best practice in the offline world. This would link to the planned Police Central Unit (being led by the Metropolitan Police on behalf of ACPO) and the plans of the Serious Fraud Office. This approach now had support from the Government, particularly from Ministers at the Home Office and Department for Business. The consultation workshops at the pre-IGF Consultation Conference, hosted jointly by Nominet and the Department for Business the previous week, had shown equally strong support from industry and NGOs. A straw poll had also indicated that security was by far the highest priority for intra-UK action, although access and openness were seen as equally important when looking at priorities for International action. See [www.nominet.org.uk/about/bestpracticechallenge](http://www.nominet.org.uk/about/bestpracticechallenge) for the feedback from the Nominet workshops and details of the Nominet Best Practice Awards which were announced at the same event and presented by the Minister of State, Rt Hon Stephen Timms MP).

Professor Michael Levi said we needed to base policy on proportionality and rationality and reduce the risk of poor choices being based on imperfect information. We needed a calmer debate on ID Theft/Fraud and more clarity in its difference from pre-existing ‘card present’ fraud. Two thirds of detected criminal activity on-line was fraud but, overall, the interface between fraud and “e-crime” was over-hyped: most large frauds were dependent on e-dimensions mainly for routine funds transmission rather than for commission. The situation would be very much worse if criminals had a better understanding of the technology and the structures of the information society. We needed to minimise their rate of exploitation of e-opportunities at various stages of the organisation of crimes. He commented on the different objectives of overlapping recording and reporting structures, such as those of APACS and the Police. In the media and public’s mind this could lead to double counting and neglect the human impact of even frauds that were compensated financially. Humans would still be needed to collate information and support consumers as fraud victims.

Charles Cox (EDS) agreed with the need for collaboration but struggled with the concept of Internet Crime. We do not refer to “path crime” even though most burglars approached houses via the path. We are dealing with criminals making use of technology to commit old crimes and our legacy of insecure Cobol systems is at least as big a vulnerability. We need to distinguish between the interception of transactions and copying of stored information. We

also need to consider the rate of change in technology convergence and of user behaviour. Trying to respond to a single concept of the Internet looks wrong. We should also consider the concept of disconnectivity, i.e. systems that only connect when they have a need. Reversing the drive to always-on may be a better way of managing and reducing risk. There is no magic bullet, no single regulatory answer. We need a composite approach. He used the analogy of fluid dynamics.

Emily Taylor (Nominet) noted that the debate seems to have moved on in recent months: a consensus view is emerging that a partnership approach to online security is necessary. This is a welcome development, and marks a shift away from the previous finger pointing and buck-passing. There is also a shift in thinking about e-security – appropriate responses have to take into account not just technology, but social and economic behaviours as well. There is no such thing as e-crime, but rather there are existing crimes committed on the Internet. Blackmail, threats to kill and fraud were still blackmail, threats to kill and fraud when they were done on-line. We needed to focus on what works. She cited the approach of the Internet Watch Foundation and the education programme being run by BEBO. However, what works in the UK may well be different to what works in other states and the same tools (e.g. filtering) may be used for very different purposes. We need to retain a sense of proportion and look at the parallels in the real world.

Charlie McMurdie (MPS) said that the “e” aspect is an integral part of virtually every crime and the policing response needs to be mainstreamed to provide an effective service and law enforcement need the skills to handle it, and to record the “use of computers or telephony to facilitate crime”. A holistic centre working in alliance with partners was needed to help overcome resource constraints. We need more co-operation on prevention but we also need more on enforcement. There was a distinction between reporting and notification (for intelligence purposes). We do not need 10,000 more incident reports. Instead we need to know the role that the Internet plays in mainstream crime.

### **Contributions from the floor**

David Lacey (former Head of Electronic Security Royal Mail, member of the Jericho Group) welcomed the call for a partnership and asked “how should we get from here to there?”

Richard Clayton (specialist advisor to the recent House of Lords enquiry into Personal Internet Security but speaking in his personal capacity) said that we needed to get the incentives right. We needed to place liability with those who are in a position to make a change. We need to stop the criminals from making money and/or catch and prosecute them wherever they are. We need joined-up approaches to international action.

Rick Chandler (EEMA and IMIS Council member) In the electronic world the “Police” often have evidence as to where criminal material or software resides (e.g. Corporate Servers) but are restricted by legislation or lack of resources from exploiting their knowledge. In the physical world they have powers to enter and secure a property and give support to the owners in subsequent litigation if they do not have resources to act themselves. Companies have huge resources and would possibly take Civil action if the Police supplied evidence (thus easing pressure on Police resources).

John Colley (CEO EMEA for ISC2) We do not make enough use of Information Security professionals. ISC2 was providing CRB checked volunteers to help child safety education programmes. We need more, similar, programmes.

Andrew Hardie (IMIS, consultant) asked whether the insurance industry was represented in the discussion. Are they not a key point of leverage?

Roland Perry (Secretary Internet Crime Forum) said that according to RIPA there are a great many law enforcement and regulatory organisations and public authorities with investigatory powers, such as trading standards officers. Where do they fit in? He was trying to create an e-victim support operation, complementary to Get safe Online and the plans for a Police Central Unit, using the Internet traditions of “create it, then grow it”.

Tricia Drakes (ex-banking software, former board member ICANN, Past Master WCIT, chair ISOC-UK, Chair 2006 Lord Mayor's Technology Advisory Group) looked to see co-operation between EURIM and the new WCIT Security Panel which she chairs. The "leave things as they are" (or the "American solution" as referred to by Alun Michael) is already an international partnership. ICANN is a not for profit privately funded "co-operative" with the majority of its leadership and participants being non American (including its Board of which over 80% are non-American). We need to take ICANN seriously and encourage greater participation (including by Industry). The weakest link in security is the "human factor", including individuals, organisations and government. Institutions without security policy and/or security awareness fail in their role in supply chains – for example the Land Registry is a serious point of vulnerability. [Note action has since been taken]. But we need to retain a sense of proportion, and be mindful of the "80% of the benefit is usually available for 20% of the effort" rule. We need to consider introducing a "CyberNeighbourhood Watch".

Unknown: we are too passive. We need to track phishermen: watch, act and trap

Unknown: unhappy about the discussion over liability. if we are burgled we do not ask the locksmith for our money back nor do we report to a national centre.

### **Wind up comments from the panel**

Michael Levi said that notification and reporting systems needed to reflect the action that would be taken by participants. He also noted that the privatisation approach of units like the Dedicated Cheque and Plastic Card Unit was anathema in other countries.

Charles Cox referred to the growth of content-driven crime but was cautious about new structures just because the technology being used to commit old crimes was changing.

Emily Taylor said that we should demonstrate how partnership works in the UK as a first step. The Internet Watch Foundation was an excellent example and the Nominet best practice awards [www.nominet.org.uk/about/bestpracticechallenge](http://www.nominet.org.uk/about/bestpracticechallenge) had successfully identified other examples for showcasing at the IGF in Rio de Janeiro.

Charlie McMurdie referred to the National Fraud Reporting Centre. Law enforcement was intelligence rich, resource poor. We need to consider who can/will act on the results because it was not necessarily the police. It was often easier to follow the money trail than the IT trail. The prime function of the central unit was to increase the ability to respond.

Alun Michael referred to the impact of the North Wales Coast road rather than the path to your front door as an example of the need to change both crime prevention and police approaches. This had forced Merseyside and North Wales Police to co-operate more closely as criminals exploited new opportunities. We need to deal with e-Graffiti in order to halt the erosion of confidence. He also referred to the use of hospital accident and emergency records not only to identify previously unreported crime but also to target the remedial action necessary. The problems cannot be left to government and law enforcement, but they had to be part of the solution. Governance had to include Parliament across parties and civil society to underpin a partnership approach – but there had to be a lead and drive from industry. The alternative was to leave it to Government, and a top-down legal/bureaucratic approach would be bad for business and for users of the Internet. If the report back was positive, we would need to be in a position to move rapidly after the IGF.

Footnote: Later in the Conference Nicholas Negroponte said that for all the increases in power, PCs today were slower than 5 - 10 years ago because of "obese" software. The "one-per-child" laptop was faster and more secure than most laptops because of its use of stripped out, open source software (though it has a slot for a card to run windows and three USB ports instead of the normal two for other add-ons). By being low energy, it could be driven by "child power" through a crank, allowing use even where there was no power source.

**Report posted by Philip Virgo, 12/11/2007**