EURIM Consultation Response

January 2004

THE EUROPEAN INFORMATION SOCIETY GROUP EURIM

Policing: Building Safer On-line Communities Together
EURIM response to the Home Office Police Reform White Paper

Introduction

EURIM is an all-party parliament industry group concerned with the politics of the Information Society. It has over a hundred parliamentary members (including Ministers and Front Bench Spokesmen) and over seventy corporate and associate members as well as over a hundred observers from Government Departments and the Public Sector. Because of the timescale it has not been possible to go through our normal membership consultation. This response is based on the work of the team working on the EURIM - IPPR study to help set the agenda for a national strategy for addressing E-Crime.

The response is structured with an initial preamble, which gives the background to the response, followed by a summary of key points. There are two supporting appendices. One is the discussion paper launched in December, summarising the conclusions from the first phase of the EURIM - IPPR Study. The other is the report of a workshop to discuss possible responses to paragraphs 4.19 - 4.21 of the consultation paper. As will be clear from that report, we have only "scratched the surface" of the issues that will need to be addressed and would be pleased to help with more detailed consideration of the options.

Preamble

The forward to the consultation refers to the need to "empower local communities to engage in the common endeavour of beating crime". More than half the population of the UK are now regular users of the Internet, as is over 10% of the population of the world. So too is a similar proportion of criminals. The criminals are using the technology to commit old crimes more efficiently and to commit new ones. At the Crime Science conference, organised by the Jill Dando Institute in November 2003, over 200 delegates, mainly from law enforcement, were told by Nick Ross (Crimewatch) how traditional crime broadly splits into:

- opportunistic crime - committed by those who are lazy or mischievous - which can be greatly reduced by the simple precautions, visible deterrence, the fear of detection and the application of scientific method to designing out vulnerabilities;

and

- organised crime - committed by those for whom it is a business and who are often in advance of law enforcement in the application of technology - this is far harder to deter and commonly requires intelligence led policing to unravel and address.

In the electronic world we can see a similar pattern emerging and the result threatens to overwhelm the ability of law enforcement to cope.

The Internet has been described as "The Wild West without six guns". But the involvement of organised crime means that many of those behind the current wave of denial of service attacks (the on-line equivalent of traditional extortion rackets) and "phishing" expeditions (some precisely targeted, others mass-market) are deploying very much more effective tools than the six-gun to achieve their objectives. Meanwhile the investigatory backlog mounts.

The Wild West was tamed by Pinkerton Men and Vigilantes because traditional law enforcement could not cope. If we wish to preserve our traditions of democratically accountable policing we need to move rapidly to ensure that UK law enforcement can.

But the current disparity between the electronic security and investigations budgets of law enforcement and of industry is even greater than that during the decade of so after the American Civil War between those of the Sheriffs and Deputies and of the Banks and Railroad Companies. The total funding available to the NHTCU (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.

Meanwhile, if more funding were to be made available for public law enforcement there is a widespread impression that the majority of voters would prefer to see it spent “putting bobbies on the beat, not skulking in offices behind computer screens”. The exception is with regard to the apparently rising tide of paedophile activity over the Internet, linked in the public mind with the pornographic spam supposedly filling the e-mailboxes of their children and grandchildren, even if the parents and grandparents are not themselves on-line to see it.

Here we need to contrast the resources available to the Internet Watch Foundation and to UK police forces for investigations like Operation Ore, with the 600 or so trained “silver surfers” (drawn from the pensioners of both law enforcement and the ICT industry) who help the American equivalent and 400 or so FBI officers handling the investigations they have helped launch. We can also contrast the UK approaches to the provision of active filtering and protection for schools and the vulnerable with those of nations like Australia and Canada, which are leading us into the on-line world.

In this area there may be strong support for a change of scale in the resources deployed by law enforcement to actively investigate and prosecute more of that which is already reported, as well as to remove barriers to what suppliers can do to protect their customers, including parents and children as well as small firms, primary schools, play-groups, study centres, after school clubs and other “businesses” with little or no budget for ICT, let alone security, support.

This raises issues of skills and governance which will require inter-departmental co-operation, not just with DTI and DfES but also all those departments, agencies and regulators with investigatory powers or at risk from computer assisted fraud. The solutions will also require funding. There is a clear desire to reduce the cost by involving volunteers but, even if this is successful, most will have some but not all of the skills and experience required and will need training. Even those who do not need training will need basic vetting. They may also need more advanced vetting if their skills are to be most effectively used.

The first appendix to this submission concludes that we need a major consultation exercise “structured in such a way as to bring the necessary players together, across organisational boundaries, to identify and recommend solutions that will work”. Such an exercise will need serious funding but will cost far less than ineffective, or perhaps even counter-productive, policy. It also needs to be joint, across departmental boundaries, as with the “21st Century Skills” consultation, led by DfES but signed off by the Prime Minister, Chancellor and three Secretaries of State.

The second appendix to this submission focuses on the some of issues that will need to be addressed if we are indeed to harness industry and voluntary resources in support of law enforcement in the fight against computer-assisted crime.

EURIM would be pleased to help organise practical follow up in both areas.

Summary of Key Points relating to Specialist Constables (4.19 - 21), Civilian Volunteers (4.22) and Lead Forces (6.10)

ICT has long been a career for those who are mentally, but not necessarily physically, able. Moreover, few of the experienced ICT professionals who volunteer to assist programmes such as IT4Communities are aged under 50. Current UK police frameworks allow for the employment of the disabled and over 55s as part-time professionals but not for their use as volunteers. While it is possible to make recommendations within existing legal frameworks, there is a need to consider whether some of the constraints are really necessary.

If the shopping mall, housing or children's playground would benefit from a "Community Support Officer" with limited powers, acting as a visible deterrent and as the eyes and ears of law enforcement,capable of acting as a professional witness, would not a similar approach be appropriate for Internet auction sites, discussion groups and chat rooms? And does the "virtual community support officer" need to be physically able to walk, let alone run?

Each year, several thousand women ICT professionals leave the ICT industry because they cannot combine the employment opportunities on offer with the need to fund care for their children or, increasingly, for elderly relatives. Over the past three years, somewhere over 100,000 men have also left the ICT industry as jobs have been lost or moved overseas. The market has (most recent quarter) shown a modest upturn, but many individuals have neither the skills in current demand nor the opportunity to acquire or demonstrate them other than by undertaking semi-voluntary roles providing computer support to schools or charities.

A number of the models used in other countries do not fit with the current UK policing environment and there are concerns over political and social acceptability, as well as legal and administrative practicality. However, there is growing pressure for action. Moreover, industry, especially financial services, is bearing the cost when similar "grooming", alias "social engineering", techniques are used to inveigle account information and personal details from mature customers to bypass electronic security. Their losses and the tax revenues lost to the exchequer, may already be considerably greater than the cost of effective action.

This will not be an easy area to address. The moment one moves outside current UK frameworks, deficient though they may be, there is a need to address issues of governance and liability, let alone responsibility for the costs of vetting and training. There is also the equity and practicality of expecting one individual to do for free that for which another might charge £100 an hour (or more) given the shortage of specialist skills in some areas.

The participants in the EURIM-IPPR study therefore recommend a step by step approach: beginning with that which can be done within existing legal and administrative frameworks, then making extensions for which there is widespread support while, in parallel, consulting thoroughly on those recommendations which entail major change.

The first steps should include pilots to test the practicality of:

registers of experts on whom law enforcement can call for technical assistance under existing governance arrangements. The organisation, promotion and administration of such registers is a non-trivial task and will need funding, including for vetting and updating arrangements. There are also issues of liability, including for experts "volunteered" by their employer to provide support, which might or might not be professionally charged.

routines for Internet specialist constables akin to those now being piloted for fraud specialists. These might initially be established for those experts with whom police will wish to share operational information, or who may be asked to assist with the gathering and analysis of evidence, as opposed to "merely" helping with technical support. It should, however, be noted that success will be limited until some of the deficiencies in the current model have been addressed because many of the industry security experts most likely to volunteer would find it difficult to meet current physical fitness requirements.

multi-disciplinary Internet Crime units, staffed jointly by secondees from law enforcement and from industry, akin to those addressing card and payment fraud, to address specific types of Internet Crime (e.g. grooming, phishing, denial of service linked to extortion). The success of the existing units raises, however, many questions, including of funding, accountability and priority setting. These need to be openly discussed and possible solutions tested.

We also need to ensure that the **business plans for the Criminal Justice Sector Skills Council address how to develop, assess , and accredit the investigatory and forensic skills needed.** The plans should be designed to cover not only full-time law-enforcement professionals and support staff, but also registers of experts, specialist constables and civilian volunteers as well as Multi-disciplinary industry-law enforcement teams. They should be designed to cover the relevant in-house skills of industry in ways which facilitate sharing the costs of developing and delivering good quality courses and materials which are directly relevant to the audiences concerned. They must be trained and co-operate, and the cost of good quality courses and materials shared.

In parallel, we need to explore the potential for greatly enlarging the pool of volunteers available, but under governance routines that are acceptable to all concerned, including the Courts.

We also need to look at the use of part-time professionals, perhaps on similar terms to those for interpreters or police surgeons.

Among the areas which might be explored are:

limited warrant special constables, so as to make more effective use of industry security professionals who are not physically fit to perform the traditional duties of a constable or who may have constraints on their availability or suitability (including for commercial reasons).

virtual community support officers whether or not they are full-time, paid or physically fit, perhaps with special arrangements to attract women returners, computer science students, silver surfers. Such groups could help with monitoring chat rooms and some of the more labour-intensive track and trace tasks that are currently not being undertaken.

international investigation teams: global organisations (banks, oil companies, airlines and ICT infra-structure suppliers) often have more experience of handling cross-border attacks and threats than most law enforcement agencies, but the means of tapping that expertise appears very limited.

We recommend monitored pilots to build confidence.

The attached appendices develop some of the ideas above in more detail, particularly the creation of registers of volunteers. Those concerned would be pleased to help explore these ideas further, including perhaps with the organisation and implementation of pilots.

Appendix 1: Partnership Policing for the Information Society

Appendix 2: Summary Report of the meeting of the EURIM-IPPR E-Crime study group on possible EURIM response to the Police Reform White Paper, held on 15 January 2004