



Building Communities, Beating Crime
A better police service for the 21st Century
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. Over the past two years EURIM has been co-operating with the Institute for Public Policy Research on a study into the actions needed to enable law enforcement to respond effectively to the challenges posed by the rapid growth in the use of electronic technologies by criminals at all levels.

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. The first is the paper produced in direct response to the Police Reform White Paper statements on the need for more work on “non-geographic crime”. The second summarises those involved in the EURIM – IPPR study.

Preamble

Paragraph 5.99 of the White Paper says that Government wishes to explore “the creation of dedicated teams across regions or groups of forces with the specific task of co-ordinating the effort against level two criminality in that region or area.

Paragraph 5.66 adds that “Government will explore the further development of arrangements for lead forces or specialisms, in particular for those crimes which, by their very nature, are not confined to geographical force areas – such as high tech crime or online paedophilia.”

The implication is that the use of the Internet or Computers to identify, contact and exploit potential victims is “special”. But over half the population of the UK now uses the Internet. So too does a similar proportion of criminals. The cost of computer theft and fraud (losses and prevention) is said to have already outstripped that of physical theft. The investigation of physical crime increasingly entails the analysis of digital evidence, such as that from the mobile phones and computers of victims and suspects or the surveillance cameras covering relevant locations.

The criminals are using the technology to achieve economies of scale in committing old crimes more efficiently, to invent new ones and to confuse law enforcement. Meanwhile less than a thousand UK police officers and support staff have been trained to secure basic digital evidence and less than a hundred have the skills and availability to analyse such evidence and present the results in court for civilian (i.e. excluding anti-terrorism) law enforcement.

The lack of priority given to ensuring that UK police forces have the resources, expertise and structures to handle the rising tide of electronically assisted crime at all levels, from localised anti-social behaviour (e.g. text bullying in school or cyber-stalking) through to organised international crime (e.g. extortion attacks on major financial institutions or mass-market phishing) is commonly blamed on the failure of attempts to measure the impact of computer crime. These failed because of the assumption that computer crime is “special” and can/should be reported separately. Most activities requiring digital expertise on the part of those responsible for prevention, investigation and prosecution use computers instead of (or alongside) guns, crowbars and motor vehicles to commit old crimes.

There is a need for a national strategy to handle the consequences but that strategy needs to be in the mainstream of traditional policing, not a specialist add-on.

The Organisation of Internet Policing

The needs are

- to provide our traditional law enforcement agencies with adequate resources and effective processes to handle e-crime and digital evidence within their own boundaries;
- to provide and resource effective frameworks and processes for co-operation across boundaries (law enforcement, regulatory, technology and industry as well as local, national and international);
- to provide and resource effective frameworks and processes that enable law enforcement agencies to help lead partnerships with regulators, industry and individuals to protect those at risk and to enable victims to report incidents to those who will take action and help them obtain redress.

Given the current lack of resource and expertise and the rate of change, restructuring is likely to be counter-productive.

Instead the need is for step-by-step progress, building on existing structures, to create the Internet equivalent of community policing.

This needs to include:

- Non-geographic Internet crime and disorder partnerships (CADDIES) supported by a shared secretariat and joint (law enforcement and Industry) investigatory teams.
- A central reporting and information clearing service for Internet (and other non-geographic) incidents, which also publishes guidelines on investigatory processes and what to report to whom.
- Routines for the accreditation of industry staff and civilian volunteers to work alongside law enforcement in joint investigatory and prevention teams, local, national and international.
- Democratically accountable third party governance routines for non-geographic policing that are at least as credible as those for traditional geographic policing.

Above all, however, it requires that UK local and regional police forces have the in-house skills and resources to help lead investigations which may require co-operation across all types of boundary, criminal, civil and regulatory as well as local, regional or international.

The scale and nature of cross-boundary co-operation needed and the different priorities of the communities whose support will be needed means that the central secretariat and reporting structures will also need both serious resource and credible public accountability.

[Appendix A](#) is the paper produced as part of the EURIM - IPPR study in response to the White Paper. The other five discussion papers on the EURIM website www.eurim.org.uk are also relevant.

Appendix B lists the participants in the study.

Appendix B Participants in the EURIM IPPR E-Crime Study

Approximately 200 individuals from over 80 organisations have been registered as participants in the EURIM - IPPR study which has comprised over twenty workshops, plus routines for contribution by e-mail, to compile, discuss and review evolving discussion papers.

The objective has been to collate and summarise inputs from those with relevant experience and expertise and identify recommendations that command consensus support.

The EURIM corporate and associate members employing those registered as participants in the EURIM - IPPR study included: APACS, Aviva, Barnardo's, BCS, BP, British Music Rights, BSI, BT, Cable and Wireless Camelot, Cisco, CMA, Computer Weekly, CPHC, EDS, Energis, Experian, Fujitsu Services, Herbert Smith, IBM UK, IEE, IMIS, Intellect, (ISC)², Legal and General, LINK, LINX, LogicaCMG, Microsoft, PCG, QinetiQ, RBS, Reuters, Royal Mail, SOCITM, Symantec UK, The Corporate IT Forum – tif, Time Warner, VNU Business Publications, Vodafone and Wanadoo.

The organisations employing those registered as observers and guests for the EURIM – IPPR Study included: Anite (now in the process of joining EURIM as a Corporate Member), Cabinet Office, CBI, Centre for Commercial Law Studies, Common Information Environment, Crown Prosecution Service, DTI, e-Government Unit, e-skills UK, Financial Services Authority, Forensic Science Service, Greater Manchester Police, Home Office, IAAC, Identrus, IoD, Internet Watch Foundation, Jill Dando Institute, London Chamber of Commerce, London School of Economics, Metropolitan Police, Ministry of Defence, NHTCU, NISCC, NSLEC, Office of the Information Commissioner, Oxford Internet Institute, Philippsohn Crawfords Berwald, Portsmouth University, P.O.S.T, Siemens (now in the process of joining EURIM as a Corporate Member), Skillset, Skills for Justice, SSDA, St Pauls Chambers, TelecomsAdvice, The Open Group, TUFF, UKAS, UKERNA and the US Embassy.

The workshop chairmen, rapporteurs and editors included: Chris Devine, David Harrington, Chris Sundt, Philip Virgo, Jeremy Ward and David Wright.

The study also had political monitors drawn from the three main parties. These included five members of the House of Commons and two members of the House of Lords.