

## Technical Appendix to Annex 5 Cyber-Crime Investigation and Enforcement

### 1 Background

In January 2005, [www.eurim.org.uk/activities/ecrime/050131submission\\_PoliceReform.pdf](http://www.eurim.org.uk/activities/ecrime/050131submission_PoliceReform.pdf) EURIM responded to the Home Office consultation “Building Safer Communities Together”, particularly the sections on Specialist Constables, Civilian Volunteers and Lead Forces. with a call for pilots to test the practicality of registers of experts, routines for Internet special constables and multi-disciplinary Internet Crime Units. Among the areas where it called for further work were “limited warrant special constables” (to make use of those with limited availability or not physically fit for the office of constable), “virtual community support officers” and international investigation teams, enlisting the expertise of multinationals corporations in working with law enforcement around the world. That paper also commented 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 (created in 2001 to investigate serious and organised crime over the Internet and to provide funding, co-ordination and back-up to computer crime units to the 43 police forces of England and Wales) moved across to the E-Crime Unit of the Serious and Organised Crime Agency [www.soca.gov.uk](http://www.soca.gov.uk). Earmarked funding and central support for the computer crime units ceased but SOCA had more than twice the resource for addressing what had taken up most of the time of the NHTCU staff - albeit not that which had the most public image. Hence the controversy over the demise of the NHTCU, despite a more than doubling of spend.

That controversy led to a proposal for a National E-Crime Prevention Centre [www.necpc.org.uk](http://www.necpc.org.uk) to take on the NHTCU crime prevention and in 2007 it was agreed the Metropolitan Police would be the lead force on E-Crime and the City of London Police would lead on Fraud. The Metropolitan Police are currently seeking funding (including from the private sector) for a Police Central E-Crime Unit (see appendix) that will work closely with SOCA, the City of London Police and a new National Fraud Reporting Unit.

In the meantime industry has perceived (correctly or otherwise) an apparent decrease in the number of police officers and support staff addressing Internet related crime, other than with regard to child abuse. The House of Lords [www.publications.parliament.uk/pa/ld200607/ldselect/ldscitech/165/165i.pdf](http://www.publications.parliament.uk/pa/ld200607/ldselect/ldscitech/165/165i.pdf) therefore “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” and 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 that happens, the policing of the on-line world, as with that of the railways in the 19<sup>th</sup> Century, is being conducted and funded almost entirely by industry, whether to protect its infrastructure from theft or terrorism (c.f. the police forces of the Railway Companies investigating Fenian and Suffragette attacks on signal boxes and stations) or its customers (c.f. protecting passengers and guarding goods in transit). The limitations of such an approach were already apparent by the 1890s when the hot pursuit after a theft at Kings Cross station crossed half a dozen policing boundaries and court jurisdictions. Moreover, by the time the British Transport Police were created the railways accounted for more than half of all reported theft.

### 2 Law Enforcement and Regulatory Agencies, including joint units

The E-Crime section of the Serious and Organised Crime Authority [www.soca.gov.uk](http://www.soca.gov.uk) has an establishment of about 80 staff (although there are alleged to be rather fewer experienced officers and specialists currently in post). It 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.

The Metropolitan Police is the lead force on e-crime and the Computer Crime Unit within Economic and Specialist Crime Command Unit [www.met.police.uk/about/organisation.htm#sc](http://www.met.police.uk/about/organisation.htm#sc) is one of a number of units handling e-Crime within its Specialist Crime Directorate: not to be confused with Special Operations (alias SO12, the “Special Branch”) which has its own team within SO15 (The Counter Terrorism Command) for monitoring the on-line activities of terrorist groups. The Child Abuse Investigation Command also has its own Hi-Tech Crime Unit and works closely with CEOP (see below)

The Economic and Specialist Command Unit (originally established in 1946 as the Fraud Unit) leads on economic crime, high tech crime, proceeds of crime and human trafficking. The computer crime unit (about a dozen officers) is focussed on offences committed under the Computer Misuse Act, primarily hacking, denial of service and the creation of malware. Separate teams, including those working via Operation Sterling, address ID theft and fraud, including against the local authorities in London (each with an embedded police officer). Other teams include the Film Piracy Unit, run in partnership with the Federation Against Copyright Theft (see below) and the Dedicated Cheque and Plastic Crime Unit (DCPCU) [www.dcpcu.org.uk](http://www.dcpcu.org.uk). The DCPCU is fully “sponsored” by the banking industry and resourced by APACS and its members, who provide fraud investigators and administrators to work alongside police officers and civilian staff from the City of London and Metropolitan Police. The DCPCU also has a national remit to tackle the organised criminal gangs responsible for the majority of cheque and plastic card crime in the UK.

The Child Exploitation and Online Protection Centre [www.ceop.gov.uk](http://www.ceop.gov.uk) “works across the UK and also maximises international links to deliver 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 Information Commissioner [www.ico.gov.uk](http://www.ico.gov.uk) can and does take action in the event of breaches of the Data Protection Act but his resources are limited. Although the legislation allows for unlimited fines, the penalties to date have rarely been more than a few hundred pounds. By contrast the Financial Services Authority [www.fsa.gov.uk](http://www.fsa.gov.uk) fined the Nationwide Building Society £980,000 for not having adequate controls in place when a laptop containing unencrypted customer details was lost/stolen.

ICSTIS [www.icstis.org.uk](http://www.icstis.org.uk) the premium rate services regulator has a remit to act when Internet scams involve the use of premium rate phone-lines. Some of these have been closely linked to the UK-based customers of multi-media phishing and spamming operations.

Over 300 agencies have investigatory powers under the Regulation of Investigatory Powers Act and other legislation. Many of these, 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. Others do not, despite reports from the banks that those who attempt to defraud them using multiple and/or fictional identities also use these to support systematic benefit fraud,

### **3 Industry Groups and Players**

The Internet Enforcement Group [www.ieg-uk.org](http://www.ieg-uk.org) is a cross industry body of Internet investigators representing the book publishing, music, games, software, merchandising and firm industries. Its members are the BPI [www.bpi.co.uk](http://www.bpi.co.uk) for UK record companies, ELSPA [www.elspa.com](http://www.elspa.com) for the UK computer games industry, FACT [www.fact-uk.org.uk](http://www.fact-uk.org.uk) for the UK film and satellite television industry, MCPS [www.mcps.co.uk](http://www.mcps.co.uk) for UK music publishers, FAST [www.fast.org.uk](http://www.fast.org.uk) for business software publishers, The Publishers Association [www.publishers.org.uk](http://www.publishers.org.uk) for book, journal and electronic publishers and BBC Worldwide [www.bbc.co.uk](http://www.bbc.co.uk), the commercial subsidiary of the BBC. Their members organise and fund almost all investigations into on-line piracy and intellectual property theft in the UK, whether these lead to criminal prosecutions involving the police and/or trading standards officers or to civil action.

The main telecoms players support TUFF [www.tuff.co.uk](http://www.tuff.co.uk) (the Telecoms UK Fraud Forum) and MICAF [www.micaf.co.uk](http://www.micaf.co.uk) (the Mobile Industry Crime Action Forum). These share offices and staff, have overlapping memberships and address issues of investigation and detection as well as of prevention through sharing of best practice and training. Their members, in co-operation with the main Internet service companies, provide the technical expertise and support for tracking criminal communications of all types, from “traditional” telephone tapping through tracing mobile traffic and to current attempts to trace e-mails and voice over IP in “real time” as well as in arrears.

The main banks and financial services players collectively support units like the DCPCU via APACS, the British Banking Association (which recently passed its anti-fraud operations to APACS) and the Finance and Leasing Association [www.fla.org.uk](http://www.fla.org.uk). Many also have in-house fraud investigation teams of similar size to the DCPCU, (some very much larger), working alongside even larger information assurance, governance and fraud prevention teams. And almost all serious fraud is now computer assisted, albeit most really serious incidents also involve insiders.

The UK-based investigation teams of the multi-nationals in industries such as pharmaceuticals, aerospace, oil and gas tend to be smaller, with the in-house security effort focussed mainly on governance and prevention and with major investigations commonly contracted out to organisations with national and international investigation and law enforcement liaison expertise: such as Control Risks, Deloitte, Detica, IBM, KPMG, Kroll, LogicaCMG, Qinetiq, Siemens Insight etc. Thus one global anti-piracy investigation organised through the City of London police by such a supplier, was said to have cost the victimised aerospace company over ten million pounds, including to reimburse police costs, but enabled it to retrieve all of that and more in damages.

Some of the major suppliers also undertake pro-bono investigations on behalf of groups of small customers and/or end-users. Thus Microsoft recently obtained £50,000 in damages and costs from a UK spammer - over ten times the largest fine yet levied for abusing personal data. In the US similar actions have led to multi-million pound settlements.

#### **4 Current Initiatives - Specialist Units and Specialist Constables**

The second appendix to the EURIM response to the Home Office consultation “Building Safer Communities Together” [www.eurim.org.uk/activities/ecrime/050131submission\\_PoliceReform.pdf](http://www.eurim.org.uk/activities/ecrime/050131submission_PoliceReform.pdf) is a report of a meeting in January 2004 to discuss models for drawing on industry expertise: looking at these from the perspectives of both private sector and law enforcement. It found a need for ongoing commitment on both sides and issues regarding vetting, liabilities and conflict of interest. The conclusion was that the way forward was “not to jump at specific models but to test possible routines with pilots which, if successful, can be templated”. Such pilots would have, however, to be funded and monitored for the lessons to be learned and the results shared and success replicated.

One of the suggestions was for “a specialist child protection unit ...[which] ...might work with the Internet Watch Foundation and be able to draw on rings of part-time professionals, volunteers and both University and Corporate resource as well as that of different parts of Government.” CEOP has since combined both ideas. It draws on the expertise of major industry players, (like Microsoft, which also provides sponsorship and technical support for the IWF) and also uses panels of vetted industry volunteers (e.g. over a hundred from CISCO alone) to support education programmes, including via partners like Childnet International.

Another suggestion was to build on the routines whereby “The specialist accountants being recruited to the Fraud Squad have the full powers of a warranted special constable. This enables them to be given access to otherwise confidential material and to accompany the named officers on a raid without having themselves to be named on the warrant. It also gives them credibility within the police service because they are formally trained (like all special constables) in police practices and procedures such as evidence gathering and presentation and are under police governance. They are, however, appointed as warranted ‘special constables’ for an indeterminate term of office, which means that they must be under 55 when appointed and

be physically fit for normal police duties even though they are not expected to perform them.” This last condition rules out many, perhaps most, of those who are successfully used in the United States to supplement the resources of law enforcement.

Nonetheless, the Metropolitan Police is building up a cadre of Special Constables with IT expertise. This has been helped by the discovery that many of its existing “specials” work in the IT industry. The MPS is also exploring routines whereby ICT suppliers and users encourage their staff to volunteer, akin to those used to encourage the employees of major retailers to do so - and help police their shopping malls.

At least one police force is also known to be looking at e-Community Support Officers and e-Community Support Volunteers to monitor chat rooms and act as witnesses.

The “Territorial Army” model, with retainer payments and pay while on duty, does not exist in the UK police service but is also used to provide specialist investigation skills to one of Signals Regiments which undertakes overlapping tasks with regard to counter-terrorism.

By far the most important single initiative is, however, that of ACPO and the Metropolitan Police for a Police Central E-Crime Unit (see next page). This will draw heavily on industry support and work closely with SOCA, the City of London Police and a new National Fraud Reporting Unit.

**Appendix (overleaf):**

Diagram of ACPO/MPS plans for a “Police Central E-Crime Unit”

## 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 threads

SOCA Capability



## Partnership Development Unit

Identify Key Stakeholders and create structured Forums re Intelligence Sharing

Joint Intelligence Sharing Protocols to be established with Industry

Identify Funding opportunities for UK & International E-Crime Initiatives

SPOC for Internet Crime Forum and National e-crime strategic group.

National & International interface with Interpol/Europol

MOUs with external agencies re data sharing, tasking & operational terms of engagement

Joint Police and Private sector Operations

## 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  
Hate Crime  
Counter terrorism  
Hackers/Malware  
BotNet Taskforce

## Co-ordination Unit

ACPO Liaison

Media – Internal and External

National Policy Development (NeSg)

Legal SPOC for advice, co-ordination and best practice

Central Skills Database

e-crime Awareness Training

Direct & Management of law enforcement national e-crime Strategy

Performance Measurement

National and International interface with Interpol/Europol/Cepo 1 /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

