

Technical Appendix to Annex 1 Cyber-Crime Reporting and Intelligence: How do we know what is happening?

1 Background

In December 2004 "The Reporting of Cybercrime" www.eurim.org.uk/activities/ecrime/reporting.pdf was published as part of the joint EURIM-IPPR study into "Partnership Policing for the Information Society. The analyses used, www.eurim.org.uk/activities/ecrime/scale.pdf, indicated "much confusion over the scale and nature of e-crime". One of the recommendations was for joined up reporting. The Symantec Internet Security Threat Reports, see www.symantec.com/en/uk/enterprise/theme.jsp?themeid=threatreport show how the Global malware industry has grown since then and the cost to the UK is well summarised in a recent report, www.garlik.com/press/Garlik_UK_Cybercrime_Report.pdf, published by Garlik. The House of Lords www.publications.parliament.uk/pa/ld200607/ldselect/ldscitech/165/165i.pdf report on Personal Internet safety reflects a change in the nature of debate on e-Crime over the past year but still found much confusion as to the scale and nature of the problems and how they are best addressed.

The 2007 Oxford Internet Institute Survey www.oii.ox.ac.uk/microsites/oxis/, for example, indicates a high level of satisfaction with the Internet, even though: 34% had "received a virus onto their computer", 12% had "received obscene or abusive e-mails from strangers" and 7% "from people they know". The 2% who "had their credit card details stolen via use on the Internet" appears in line with experience in the physical world. Most end-users would not, however, know if their system had been infected with a virus unless it told them it was there, or whether their credit card details had been stolen on-line or via a garage or restaurant. Such figures are, therefore, of little assistance in gauging the scale and nature of e-crime. But they do help explain why the Internet community, law enforcement and government are reluctant to change priorities.

2 Why we need to know?

Most allegations of large and mounting problems come from those seeking bigger budgets and more resources. But that does not mean they are wrong. Most allegations that the problems are not serious and should be handled by their customers, come from organisations that wish neither to spend more on security nor to accept responsibility. That does not mean they are wrong either. There is no agreement on the reality.

Most of those reading this note cannot tell whether their personal system is slow and occasionally stops dead because it has been hijacked to form part of a botnet of zombies, or because their security software is scanning all traffic in and out for a myriad of known malware problems and regularly "pauses" to update its filters. Some will have turned off the spam filters (at least) to get back to acceptable performance levels, even though it means deleting ten or more spurious e-mails for every one that is genuine.

But are most of the problems we see caused by a few dozen global criminal syndicates harnessing a couple of hundred spammers and their botnet armies? And are those same botnets really available to also bring down bookmakers, banks, government departments or even the Internet itself - if the price is right?

If the authors/controllers of malware such as the "Storm Worm" http://en.wikipedia.org/wiki/Storm_Worm really can command millions of zombie computers and generate most of the world's spam and denial of service attacks, would it not be more cost-effective to put a fraction of the billions currently spent on information and communications security (by government as well as by the private sector) into international co-operation in tracking, tracing and removing them?

Should we give more priority (as called for in the House of Lords report) to re-engineering communications infrastructures and on-line systems to remove bottlenecks and single points of failure than to adding more layers of protection against higher volumes of cleverer malware? - an intellectually stimulating and commercially profitable "arms race" for the researchers and suppliers concerned - at the users' expense.

Or has the on-line world “merely” become part of the mainstream of human life, with consumers no more vulnerable at home to cyber-mugging (ID theft and fraud) than in the street outside and with children no more vulnerable to cyberbullying in their bedrooms than in the playground? If so, do we “merely” need to “re-educate” millions of teenagers and their parents and grandparents in order to go safely on-line to buy, sell, save, learn and play?

Meanwhile more organisations are competing for budgets, to monitor what is happening and for the time of knowledgeable victims to report on their experiences, than appear interested in taking action on the reports they receive. And their terms of reference, resources and competence are varied and often incompatible.

3 A Confusion of Reporting and Intelligence Services

Most services claim broad objectives but, in practice, focus on one of six broad priorities:

- 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.

Those running the services differ in “cultural values” and approaches to security. They range from those who deal only with individuals and/or organisations they regard as “trustworthy”, through to those claiming to provide open services to all. Some find it easy to communicate with peers in other parts of the world, but not with other parts of local industry, society or law enforcement. Some are concerned mainly to protect the intellectual property rights and commercial interests of themselves and their paying customers.

4 Who currently claims to do what?

4.1 Critical Infrastructure Reporting and Response Teams

The first “Computer Emergency Response Team” www.cert.org was created in 1988, with US Defence support, at Carnegie Mellon University. There are now over 250 CERTS worldwide, some are US-based but effectively global, like the Financial Services Information Sharing and Analysis Centre www.fsisac.com:80/ and several are based in the UK, run by communications and financial services organisations. In 2003 the US Computer Emergency Readiness Team www.us-cert.gov was created as a partnership between the Department of Homeland Security and the public and private sectors: “to co-ordinate defense against, and responses to, cyber attacks on the nation”. Carnegie-Mellon now focuses on studying Internet security vulnerabilities and relevant education and training but adjacent to it in Pittsburgh is the National Cyber Forensic Training Alliance, www.ncfta.net. This provides “a neutral collaborative venue where critical confidential information about cyber incidents can be shared discreetly and where resources can be shared among industry, academia and law enforcement” – including a highly automated global incident, reporting, tracking and response operation, funded jointly by industry, FBI and Government: the current global hub for co-operation against cybercrime.

Last year the UK public sector CERT, Unified Incident Reporting and Alert Scheme (UNIRAS) was one of the organisations, including the National Infrastructure Security Co-ordinating Centre (NISSC), that were merged to form the Centre for the Protection of National Infrastructure www.cpni.gov.uk This interfaces with those businesses which operate parts of the critical national infrastructure, the Police National Counter Terrorism Security Office (NaCTSO) and a network of specialist police “Counter Terrorism Security Advisors. Until that merger UNIRAS and NISSC were creating a UK network of geographic and sector “Warning Access and Reporting Points” (WARPS) www.warp.gov.uk The CPNI is now working with the “National E-Crime Prevention Centre” www.necpc.org.uk based on the University of Wolverhampton on WARP development for geographic and sector groups.

Many of the global infrastructure, applications and communications service suppliers (e.g. AT&T, BT, CISCO, C&W, EDS, IBM, Microsoft, UKERNA, Yahoo!), financial services and e-commerce suppliers (e.g. Barclays, eBay, Experian, HBOS, RBS) and defence/aerospace and pharmaceuticals multinationals (e.g. BAe, BP, GSK, Rolls Royce) have global incident response teams, some based in the UK, which link to the NCFTA centre in Pittsburgh.

4.2 Alert Services for large organisations

According to KEW Associates www.kewassociates.co.uk, user spend on electronic security is over £3 billion per annum. Much of this is “informed” and “supported” by services which use a variety of means to monitor Internet traffic, including for early signs that attacks are pending and on whom. These enable the vendors of anti-virus software, spam filters and other corporate and end-user protection tools to update their products and services. They also warn subscribers of vulnerabilities on which they need to take action, who may attack them (and how) and of attempts to impersonate their websites, products and services – so that they can contact domain name registrars, corporate lawyers and others to take action.

The best known suppliers of such services include BT Counterpane www.counterpane.com (including network monitoring for unauthorised activity as part of their managed security services), Symantec www.symantec.com (analyses of attacks are one of their many services offered as part of a multi-layered defence approach), Mark Monitor www.markmonitor.com (phishing attacks linked to spoof websites and intellectual piracy as part of their brand protection services) and Secunia www.secunia.com (reports of vulnerabilities in a wide variety of applications products, as part of their vulnerability management services).

4.3 Alert services for small firms, consumers and parents

IT Safe www.itsafe.gov.uk carries alerts on recently discovered vulnerabilities but its basic advice is to use the continuous updating services of the main suppliers. The NECPC www.necpc.org.uk (see above) has created WARPS (see www.warp.gov.uk for current full list) for local government, healthcare and small firms in the East and West Midlands and is working on others for schools, rural businesses, business and science parks and biotech industries. The Metropolitan Police Fraudalert www.met.police.uk/fraudalert reports the changing patterns of fraud, receiving reports from around the world as well as the rest of the UK and is due to be expanded into a comprehensive threat updating service linked to a “Police Central e-Crime Unit” - see section 5 below

The Child Exploitation and On-Line Protection Centre www.ceop.gov.uk runs an integrated service covering advice, guidance and reporting. The Internet Watch Foundation www.iwf.org.uk runs a hotline for reporting potentially illegal child sexual abuse content hosted anywhere in the world and criminally obscene and incitement to race hatred content hosted in the UK. The organisation also provides a universal ‘notice and takedown’ service to any British service provider hosting potentially illegal content within their remit.

4.4 Crime Reporting and Intelligence Services

The Internet Crime Complaint Centre www.ic3.gov is a partnership between the FBI and the US National White Collar Crime Center www.nw3c.org/partnerships/ic3.cfm. “IC3 gives the victims of cybercrime a convenient and easy-to-use reporting mechanism <https://complaint.ic3.gov/Default.aspx> that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the [US] federal, state, local and international level, IC3 provides a central referral mechanism for complaints involving Internet related crimes”. The US Federal Trade Commission runs a similar services with regard to ID Theft: [https://m.ftc.gov/pls/dod/widtpubl\\$.startup?Z_ORG_CODE=PU03](https://m.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03)

The UK has no equivalents. Current advice, www.homeoffice.gov.uk/crime-victims/victims/reporting-a-crime, refers to reporting to a police station or anonymously via Crimestoppers www.crimestoppers-uk.org. It also refers to reporting via a non-emergency notification website on www.online.police.uk. The latter is currently unavailable, pending the testing of a new system. Referrals from the US IC3 are sent to the

Metropolitan Police as the UK lead force on e-crime. The Fraud Alert website suggests that phishing e-mails be sent to reports@banksafeonline.org.uk, if they concern banks or to spooof@paypal.co.uk or spooof@ebay.co.uk. If they concern Paypal or eBay.

APACS, the UK payments association, www.apacs.org.uk runs a Fraud Intelligence Bureau (FIB) to distribute information and intelligence from the reports it receives from its members' reporting systems between the banking industry, police forces and other law enforcement agencies throughout the UK. It also runs an Industry Hot Card File (IHCF) which enables 80,000 retail subscribers to check card transactions against lost or stolen cards. There are plans to merge the FIB with the intelligence function of the Dedicated Cheque and Plastic Crime Unit (DCPCU) www.dcpku.org.uk to form a Payment Industry and Police Joint Intelligence Unit (PIPJIU). A Fraud Intelligence Security System (FISS) is under development to enable intelligence sharing between UK retail banking and card institutions and law enforcement, including the Serious and Organised Crime Authority www.soca.gov.uk, the Metropolitan Police Service and the new National Fraud Reporting Centre, NFRC. The latter is intended to bring together all reporting in this space, including inputs from CIFAS (the Credit Industry Fraud Avoidance Service) www.cifas.org.uk which maintains lists of known or suspected fraudsters so that their subsequent attempts to defraud its members (260 or so providers of credit services) can be more rapidly identified.

Comparisons between fraud reporting in the US through IC3 and in the UK through APACS suggest that the US model seriously underestimates the level and cost of incidents. IC3 reported \$198.44m losses online in 2006, whilst APACS recorded £154.5m over the same period. Anecdotal evidence from banks that have similar operations in both the UK and US is, however, that their losses in the US are several times those in the UK. There are a number of systemic reasons why this is so, including the lack of an APACS equivalent, but this suggests that 90% of comparable fraud in the US is not reported to IC3 and that suggestions the UK has higher levels of fraud and worse problems are incorrect.

The Serious and Organised Crime Agency (SOCA) liaises direct with banks and major organisations on high value cases but does not provide a reporting service except with regard to money laundering and terrorist funding. It became responsible for the Financial Intelligence Unit after the Review of the Suspicious Activity Reporting Regime www.soca.gov.uk/downloads/SOCAtheSARsReview_FINAL_Web.pdf had found (para 25) "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 www.experian.com, Equifax www.equifax.com and others run a variety of reporting and intelligence operations on behalf of financial services and insurance companies (i.e. not just credit reference services). Thus the motor insurance database (designed to help reduce insurance fraud) run by Experian can also provide more accurate, up to date and faster response to enquiries regarding vehicle details/ownership than is available via the DVLA or the "Police National Computer".

The Communications Service Providers (telcos, ISPs, mobile operators), the providers (e.g. EDS or IBM) of managed services to large organisations and some of the main banks (e.g. RBS) also run internal reporting and intelligence services, some of which exchange information with police and government services, subject to legislative and regulatory constraints, around the world. The providers of international alert and anti-malware products and services (Symantec, McAfee, Message-labs, F-Secure, Webroot etc.) have processes for monitoring traffic, collating reports from customers and exchanging threat information with each other.

Nominet, the UK domain name authority, will forward registration complaints involving .uk and has processes for handling disputes over intellectual property. Those involving overseas domains must be sent to the relevant registrar (e.g. ICANN for .com) but the routines for taking action may be non-existent.

4.6 Supplier and Industry Incident Reporting Services

Most communications service providers have routines for their customers to report malpractice. These commonly take the form of e-mailing [abuse@\[ISPname.xxx\]](mailto:abuse@[ISPname.xxx]). Bank Safe On-line also runs a collective

service for those who receive “suspect” e-mails from “their bank”: reports@banksafeonline.org.uk. Such reports commonly appear to go into black holes, although some like the phone co-op www.thephone.coop not only acknowledge receipt but reply personally. This is partly because most ISPs do not wish to show the length of their queues (perhaps several days after a widespread incident) and partly because of issues of confidentiality, but is mainly because they do not wish an ongoing correspondence if they can do nothing and the complainant feels they have done too little.

By contrast abuse@amazon.com responds with an apparently personal invitation to make a structured report via www.amazon.com/gp/help/contact-us/report-phishing.html/. Given that so many ISPs are competing on price rather than quality of service and strip overheads to the bone, the reasons for their common lack of response are clear - but so too are the consequences with regard to customer satisfaction.

There is therefore a proposal for a www.e-victims.org (currently demonstration site only) service to help victims 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 (perhaps because they are a civil matter or just an annoyance).

In many cases it will simply collect aggregate statistics regarding the number of approaches the website has received while advising enquirers that there is no need to do more than “bin” a known scam. Where incidents are reportable, it would aim to direct the victim to report to the appropriate agency, along with supporting evidence, thus reducing the need for multiple contacts before properly identifying and describing the issue. One of the objectives will be to manage expectations in line with the enforcement response likely.

5 Attempts to Bring the Scene Together

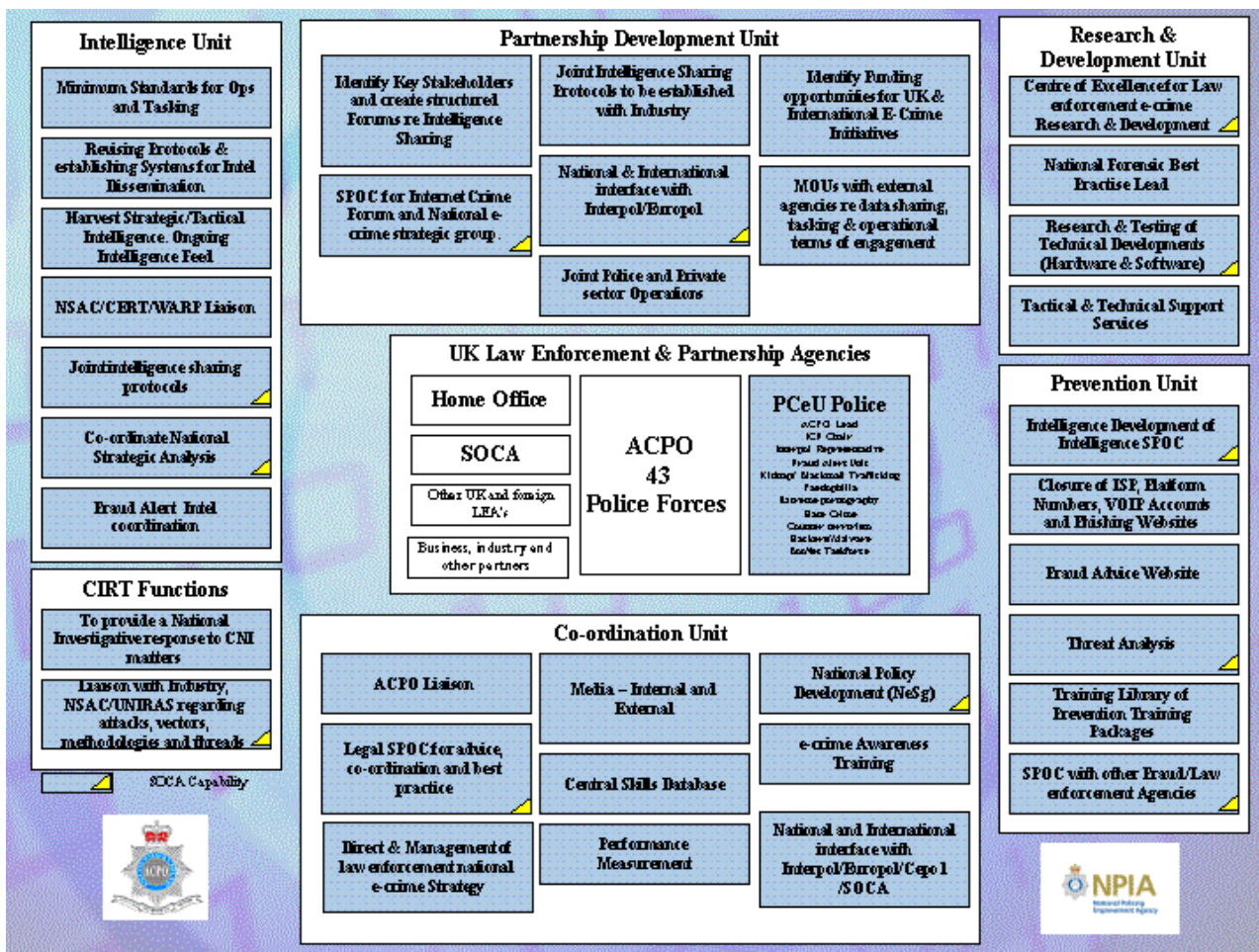
There have been a number of attempts to make sense of the situation, including to assess the scale and cost of e-crime, using a variety of definitions: the British Crime Survey now includes questions on, for example, virus attacks. But most of the so-called cyber-crime is actually traditional crime over 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 over through the letterbox, over the phone or by e-mail.

The recent Garlik report www.garlik.com/press/Garlik_UK_Cybercrime_Report.pdf is particularly helpful for listing the many sources used in its compilation of the cost and scale of E-Crime to the UK, although not how its collations and calculations were done. By contrast APACs collates only the losses reported by banks and card companies in www.apacs.org.uk/resources_publications/documents/FraudtheFacts2007.pdf “Fraud the Facts”. The trend information, some of it over a ten-year period, excludes, for example, charge backs to retailers and that written off as “bad debt” - both including unknown proportions of fraud.

The annual DTI “Information Security Breaches survey, co-sponsored by Price Waterhouse Coopers, www.enisa.europa.eu/doc/pdf/studies/dtiisbs2006.pdf collates industry estimates of incidence and cost, as opposed to reported losses. Meanwhile market research commissioned by Get Safe On-line, in 2006 showed www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf that consumers felt more likely to be victim of e-crime than of car crime, burglary or mugging. Other surveys indicate that while many respondents (perhaps most) have suffered annoyance or even losses, these were seen 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 improve the efficiency of current services, to remove tiers of delay and to find better ways of enabling rapid and trusted co-operation across organisational barriers, so as to routinely collate (automatically where-ever possible) reliable material in ways that will help target effective action.

Hence the importance of the ACPO/MPS plans for a “Police Central E-Crime Unit”, summarised in the diagram below.



There appears to be very strong industry support for such a unit to provide services equivalent to, and linked to, those of the US IC3 reporting centre and the NCFTA “reaction” centre in Pittsburgh. It is understood that both would be happy to provide their software and systems in order to improve international co-operation, using a twinned hub in a multi-cultural location like London.

There is, however, an equally strong view that the central staffing and funding must, as with the Pittsburgh centre, be via domestic law enforcement.

No-one wishes their confidential reports to be processed by a secondee training a commercial rival or liable to extra-territorial or non-judicial access.