

# **CYBER CRIME : THE CHALLENGE FOR LAW ENFORCEMENT**

## **Introduction**

Computers and the internet provide another tool for the criminal and an abundance of targets within global reach. Cyber crime concerns the use of the internet either as the means of committing a criminal offence or as a tool, hi tech crime concerns the use of computers and other communications devices. For the purpose of this presentation where the term hi tech crime is used it includes cyber crime.

It is a global problem which, though it requires global solutions must be tackled at a local level. We must also remember that hi tech crime is real crime with real victims.

All police forces must incorporate hi tech crime into their planning .At the moment cyber criminals stand to make large rewards for low risks. There is a lack of legislation and that that there is sometimes fails to keep abreast of modern technology.

There is a lack of expertise amongst the police and in places a lack of will to tackle hi tech and internet related crime; as a result the hi tech criminal stands little chance of being apprehended.

The Internet affords protection, anonymity and ease of communication

Criminals can exchange information easily e.g. chat-rooms and disseminate tools such as hacking tools or information on hacking or credit card fraud etc

Cases can be difficult to present in court due to the technical nature of the evidence and/ or the volume of material, judge's and courts may lack an understanding of hi tech crime and Sentences for hi tech crime tend to be low.

There is a lack of international co operation, safe havens from which criminals can operate from with impunity exist throughout the world.

Nowadays you do not need to be a computer programmer or possessed of a particularly high level of technical ability to commit computer crime most school leavers are now computer literate as a result this type of crime will increase

Organised Crime Groups are adept at searching out new markets to exploit and are already heavily involved in white collar crime .The level of sophistication that Organised Crime groups will employ cannot be underestimated we have seen such groups buying in such expertise where required .

## **Specific problems**

### **Jurisdiction**

Who polices cyberspace? Police forces tend to operate within their own local jurisdiction but unless someone takes on the challenge the criminal can act with impunity. These investigations take time and resources.

The international nature of cyber crime requires the ability of police and prosecutors to co ordinate cases across differing jurisdictions. This can be very time consuming and difficult, particularly in the absence of any formal instrument concerning legal co operation.

Because perpetrators may be based anywhere in the world you need to rely upon assistance from foreign states, but how do you make them care about your problem?

And, even once you find them can you extradite them or can you persuade the foreign state to prosecute?

Where offenders can be prosecuted in more than one jurisdiction does the legal process provide a mechanism to determine which jurisdiction should deal with the case?

The nature of the internet can also create difficult problems in terms of the jurisdiction of national courts.

## **Expertise**

The investigation of computer crime requires specialist skills both in tracing and identifying the perpetrator and in examining digital storage devices.

Investigators need to understand how to trace the activities of those on the Internet and how to obtain data from Internet Service Providers and Communication Service Providers. They need to know how to obtain this material quickly due to the volatile nature of much of this material, they may also need to understand that there may be restrictions on ISP and CSP in the provision of such data which may be subject to data privacy laws access only being granted once the appropriate legal threshold for its release can be demonstrated.

Investigators also need to understand how to secure evidence so that its integrity is preserved and resist evidential challenge at court. Any interference with digital data causes it to change. In order to demonstrate to the court that the data has not been changed by the investigators Police in the UK observe the following principles when seizing digital material:-

- Nothing should be done in the course of obtaining the material that alters the data in any way.
- Only in exceptional circumstances should investigators access original data ; where they do the examination must be carried out by a competent person and a full explanation given to the court
- An audit trail must be kept of the examination so that the work can be replicated if needs be.

The usual process in the UK is for the forensic examiner to utilise an imaging tool such as Encase to take a complete copy of the data and to verify the image by way of the 'hash' value.

### **Legal Instruments**

As technology moves on can the law keep up? Can you fit computer related offences into existing legislation? This can require some creative thinking on the part of the prosecutor.

### **Crime Prevention**

Policing is concerned with preventing crime as much as it is with apprehending perpetrators. Much can be done to educate the public and industry. Opportunities also exist to disrupt criminal activity and make it more difficult for them to carry out their activity; Cyberspace needs to be policed and requires an innovative approach in order to be effective whilst remaining within the law.

## **The Challenge for Prosecutors**

Whilst it is not necessary for the prosecutor to be technically proficient they do require some understanding of the technology, they need to understand where the evidence is located and to identify the appropriate charges. They will also need to understand how to obtain evidence from other countries.

Prosecutors will also need to consider the sufficiency of the evidence, much of which may be circumstantial particularly where the suspect has utilised one of the freely available programmes designed to eliminate evidence.

Because computers are capable of storing vast quantities of data the prosecutor will need to understand how to deal with this, firstly in terms of extracting the evidential material but also in relation to material that may be exculpatory or otherwise of assistance to the defendant.

In the UK there is an obligation to ensure that a defendant has a fair trial, this includes making available to him any material which may assist his defence or which casts doubt on the case for the prosecution. The court will oversee the way in which the prosecutor has discharged these obligations. However the prosecutor and the court must also ensure that cases come to court in a reasonable time and that the court focus is on those parts of the evidence that is in dispute. The quantities of data that computers are capable of storing can create a tension between these two aims. Further, problems also arise where material is not in the hands of the prosecutor but with a third party, and frequently that third party is located overseas.

## **Case Presentation**

These cases can be complex and need to be presented to the court in a way that the court can understand. The prosecutor may have to educate the court as to the way in which the technology works.

The prosecutor will have to be selective in the material he presents to the court and choose the witnesses he calls with care.

It is important that the court is presented with a case that reflects the defendant's criminality and allows an appropriate sentence to be imposed

The prosecutor needs to select the expert witnesses he plans to call with care to make sure they are capable of presenting to the court in a way which the court will understand . They will also need to work closely with the defence expert, if any, to ensure that as much of the technical evidence can be agreed as possible and to prepare a glossary of terms that are acceptable to both.

## **Case Study**

### **Operation Ore**

#### **Background**

In 1999 the US Postal Inspectorate took raided the premises of a company in Texas called Landslide Incorporated. Landslide operated a web hosting and credit card verification service for a large number of websites which predominantly offered material of a pornographic nature. By the far the most profitable part of the business

was that which offered websites containing indecent photographs of children. The owners of Landslide made significant profits from this business.

Following the conviction of the owners in 2001, the police in the United Kingdom were given a copy of the Landslide customer database. From this some 2,300 suspects were identified in the UK who were believed to have paid to access websites offering child abuse images.

The UK police then embarked on an enormous operation, the sheer numbers of suspects was almost overwhelming. Priority had to be given to those suspects believed to pose a risk to children. Search warrants had to be obtained for each and their computers examined. Where these computers were found to contain illegal material a schedule had to be prepared for the prosecutor listing and describing each image.

In order to prove the way in which a persons name came to be on the database it was necessary to send a letter of request to the USA and for UK officers to travel in order to copy the network of computers used by Landslide return them to the UK and reassemble them here , that took many months.

We also faced a number of legal challenges, including challenges to the jurisdiction of the court in the UK to deal with some of these cases.

## **Outcomes**

1. An awareness of the level of interest in paedophile material. We were staggered by the level of interest shown in this material, particularly as the database related to 1999 when internet usage in UK was at a far lower percentage than it is today.
2. This operation made us realise that our police lacked the resources and capacity to deal with hi tech crime. As a result the government made more

resources available and most forces were able to establish hi tech crime units staffed by dedicated trained officers. In due course a specialist national unit, The Child Exploitation and On Line Protection Centre was created. Similarly we realised that we had to train prosecutors and we developed a hi tech crime training course and have so far trained over 200 prosecutors throughout the country who are able to deal with a whole range of cases involving hi tech crime.

3. The courts also had to respond. Due to cases that came before the courts as part of this operation we established case law in relation to issues of jurisdiction and a structured approach to sentencing as well as other important guidance.

Russell Tyner

Specialist Crown Prosecutor

Crown Prosecution Service

Organised Crime Division London