Reform of the Computer Misuse Act 1990

ICF Legal Subgroup

30th April 2003

Reform of the Computer Misuse Act 1990

Introduction:

Concerns exist within both law enforcement and industry in respect of a number of legal issues currently being affected by advances in technology. These concerns include whether the legislative regime, primarily the Computer Misuse Act 1990 (CMA), remains fit for the purpose it was originally designed bearing in mind technological advances since its implementation.

The Internet Crime Forum – Legal Sub Group was tasked with looking at two specific objectives in respect of the CMA:

1 To focus on the continuing utility or otherwise of the CMA with particular regards to Denial of Service (DoS) attacks.
2 To assess the degree to which domestic law meets the requirements of the Council of Europe Cybercrime Convention.

Increasingly sophisticated risk analysis undertaken by both (and between) public and private sectors and the collation of statistical data (aided by the Internet) on types of crime now mean that we have a better understanding of the range and extent of criminal activity associated with computers.

It is now common to find a distinction being made between the use of computers in:

- the commission of traditional crimes
- the emergence of new ways of committing 'old crimes'
- some crimes that are context specific to, for example, the Internet
- crimes where computers are the 'victim' rather than a medium within which crime is committed.

The importance and nature of the many legislative provisions dealing both with offences and procedure that are directly affected by advances in technology were discussed within the legal sub group. It was agreed that all existing legislation and proposed legislation should be equally capable of criminalising and punishing an offence via whatever medium it is committed.

In addition to reform of the substantive law issues of procedural and evidential reform, jurisdiction and data exchange are important. Increasingly EU and other international initiatives incorporate all of these issues within a single legal framework. It should be recognised that responding to High Tech crime may involve a wide range of evidential and procedural reforms that impact on law enforcement generally.

This was recognised by Guy De Vel the Director General Legal affairs of the Council of Europe, on introducing the European Convention on Cyber crime.[1] When commenting on the relationship between the substantive law and procedure he said that:

> *"**It follows that the field of application of the procedural part of the convention is broader than that of the substantive part."***

However, other groups are already dealing in respect of such issues, for example the law commission are dealing in respect of the law of fraud, and so to prevent duplicity of work this paper is specifically aimed at dealing with questions relating to the Computer Misuse Act 1990. The Council Framework Decision on attacks against information systems as presented by the Commission of the European Communities will be binding and it is anticipated this framework will be adopted by the end of 2003, After this Member States will have two years to implement provisions into their legislation. As such the sensible option was to also consider the effects of the proposed framework on the CMA within this paper rather than treat the two as separate issues.

1 Budapest 2001

Not withstanding rapid developments in technology and the limited scope of the CMA it has proved to be a useful legislative instrument that has evolved by judicial interpretation of key terms to cover a wide range of criminal activity. However, the legal terminology/language used appears to be not only different but also distinct from that adopted by recent initiatives/proposals in the European Union and the Council of Europe Cyber-Crime Convention.

This paper therefore addresses the following questions:

Is the scope of the CMA now to limited to deal with the problems of Computer and High Tech Crime as now understood?

In so far as it can be revised/adapted is this sufficient without wider procedural and evidential reforms?

In order to consider these questions further this paper is divided into the following sections:

1. Background of the Computer Misuse Act
2. EU Proposals
3. Council of Europe Convention on Cybercrime
4. Conclusion

1 Background of the Computer Misuse Act 1990

The Computer Misuse Act 1990 (CMA) came into existence because legislation intended for other purposes did not always fit the particular facts before the court. This occurred in the case of R v Gold and Schifreen,[2]

Gold and Schifreen were hackers who gained unauthorised access to the Duke of Edinburgh's computer files contained on British Telecom Prestel Gold network. They were convicted of committing an offence contrary to section 1 of the Forgery and Counterfeiting Act 1981 (FCA) for making a false instrument. On appeal their convictions were quashed as the court said that the electronic impulses that formed the password could not be an instrument within the definition of section 8 (1)(d) of the FCA.

Although in some cases the prosecution succeeded in obtaining a conviction, as in the case of R v Whiteley[3].

Whiteley a computer hacker was convicted of criminal damage, he gained unauthorised access to a computer network and altered data contained on discs in the system, thereby causing the computers in question to be shut down for periods of time.

As a result of the problems in prosecuting such cases a Royal Commission was set up and following their recommendations the Computer Misuse Act was enacted. The English Law Commission Paper No. 186 on Computer Misuse stated that the main argument in favour of a hacking offence does not turn on the protection of information, but rather springs from the need to protect the integrity and security of computer systems from attacks from unauthorised persons seeking to enter those systems, whatever may be their intention or motive[4]. This is in contrast to the Scottish Law Commission who looked at the protection of `information'[5].

Although, the legislation was drafted before the Internet and Internet related crime became a major concern the courts have by statutory interpretation of key words managed to apply the Act to a variety of circumstances that could not have been envisaged by the original drafters of the legislation.

The CMA, as it currently stands, covers 3 distinct offences:

S1 Unauthorised Access To Computer Material
It is an offence to cause a computer to perform any function with intent to gain unauthorised access to any programme or data held in any computer. It will be necessary to prove the access secured is unauthorised and the suspect knows this is the case. *This is commonly referred to as hacking*

S2 Unauthorised Access With Intent to Commit Other Offence
An offence is committed as per S1 **but** the S1 offence is committed with the intention of committing an offence or facilitating the commission of an offence. The offence to be committed must carry a sentence fixed by law or carry a sentence of imprisonment of 5 years or more. Even if it is not possible to prove the intent to commit the arrestable offence the S1 offence is still committed.

S3 Unauthorised Modification Of Computer Material
An offence is committed if any person does an act that causes unauthorised modification of the contents of any computer. The accused must have the intent to cause the modification and be aware the modification has not been authorised. There is no necessity for any unauthorised access to have been obtained during the commission of this offence. *This offence is used instead of The Criminal Damage Act 1971, as it is not possible to criminally damage something that is not tangible.*

For a full overview of the contents of the CMA see Appendix A

[2] [1988] 2 W.L.R. 984.
[3] (1991) 93 Cr. App. R. 25, CA.
[4] Paragraph 2.11–2.15- page 11-12.
[5] Scottish Law Commission No. 106, Report on Crime, paragraph 1.37, page 7.

Perceived problems with section 3 CMA has involved denial of service attacks (DoS) and interference by authorised users of systems.

A DoS attack is a malicious attack intended to disrupt information systems, it can be committed in many ways. It attempts to overload the web servers or Internet Service Provider (ISP's) with automatically generated messages. Other types of attack can include disrupting servers operating the domain name system (DNS) and attacks directed at routers.

Statistics[6] show that there have been few CMA prosecutions and there has yet to be a DoS attack prosecution. Although section 3 CMA does not specifically refer to DoS attacks of the type now possible, its lack of precision and technology-neutral language appears to provide sufficient flexibility for such a case to be prosecuted. Such attacks are being investigated by the National High Tech Crime Unit and as with much legislation where there is ambiguity this matter may well be resolved by case law when the matters are brought to trial.

Some government lawyers (and there is academic support for their view) have expressed the opinion that any sort of DoS attack is covered by existing legislation. Section 3 of the CMA does not require unauthorised access to a computer system, merely unauthorised ***"modification of*** **the contents of any computer"**. The requisite intent that accompanies this offence is to render unreliable the data stored on a computer, or impair its operation.

However, an earlier attempt to remedy this lack of clarity came about with proposed amendments to the CMA with the:

THE COMPUTER MISUSE (AMENDMENT) ACT [HL] (hereinafter-called CMAA)

The CMAA was an attempt to suggest a limited reform of the CMA to deal with certain specified problems. The CMAA successfully fulfilled its purpose, *which was to stimulate debate*. It was not intended to cover the draft Framework Decision or the Council of Europe Convention on cyber crime. The CMAA had a number of positive features; it contained wide definitions that would cover, not just present DoS attacks but future developments in computer technology, as well as those that have taken place since 1990. It should be remembered that in 1990 when the CMA was enacted DoS attacks were not contemplated. The CMAA illustrates on the one hand the urgent need to reform the CMA but also some of the difficulties that are encountered with piecemeal reform of the substantive law.

Although having a number of positive features there are reasons why the CMAA in its present form is not a suitable amendment to the CMA:

- The Terminology used by the CMAA is like the CMA 1990 not defined in the bill. This causes a problem because the CMA 1990 referred to `a computer' and case law has been defining what that is, the CMAA changes tack completely and refers to `computerised systems' but does not state what that will comprise of.
- Section 3A(2) of the CMAA does not require intent and introduces an objective test `a reasonable person' test. This is a Caldwell reckless test and is incompatible with the liability framework contained within sections 1-3 of the CMA. A fundamental problem with this proposal is not simply whether such a test should be objectively or subjectively determined but whether a recklessness test would be interpreted alongside sections 1-3. The new section 3A does not fix any penalty for a person found guilty of an offence contrary to section 3A. Section 3 CMA 1990 at section 3(7) extends the penalty listed at section 2(5) of the CMA to section 3.
- Because the CMAA is limited in scope and was not intended to cover the draft Framework Decision or the Council of Europe Convention on cyber crime (the proposals for which are outlined below) it may be no more than a short-term solution.

[6] CMA statistics are attached.

2 EU PROPOSALS

Council Framework Decision on Attacks Against Information Systems[7]

This draft Framework Decision was introduced by the Commission in May 2002, and since this time has been discussed at the substantive criminal law working group of the European Union. The text remains under discussion, and will be adopted in 2003.

Following the eventual adoption of the text, Member States will have two years to implement the necessary measures to comply with the provisions of the Framework Decision. A Framework Decision is a third pillar instrument, which although binding as to the results it seeks to achieve, leaves the means of implementing the provisions required to the discretion of the Member States and their appropriate national authorities. Six months after the implementation date the Commission shall draw up a report upon which the Council will assess whether all Member States have taken the necessary measures in order to comply with the Framework Decision.

The approach adopted in the draft Framework Decision is in part a response to September 11 and is designed to protect critical information infrastructure security. This is understood as a defence and as both a EU/national security issue. In the EU proposal the phrase "information system" is used in its broadest sense in recognition of the convergence between electronic communication networks and the various systems they connect. Information systems include "stand-alone" personal computers, personal digital organisers, mobile telephones, intranets, extranets and, of course, the networks, servers and other infrastructure of the Internet.

Even before the draft Framework Decision was published the EU had proposed the following description of threats against information systems:

- **Unauthorised access to information systems.** This includes the notion of "hacking". Hacking is gaining unauthorised access to a computer or network of computers. It can be undertaken in a variety of ways from simply exploiting inside information to brute force attacks and password interception. It is often – though not always - with malicious intent to either copy, modify or destroy data. Intentional corruption of websites can be one of the aims of unauthorised access.

- **Disruption of information systems.** Different ways exist to disrupt information systems through malicious attacks. One of the best-known ways to deny or degrade the services offered by the Internet is a "denial of service" attack (DOS). In a way this attack is similar to fax machines being flooded with long and repeated messages. Denial of service attacks attempt to overload web servers or Internet Service Providers (ISPs) with automatically generated messages. Other types of attacks can include disrupting servers operating the domain name system (DNS) and attacks directed at "routers". Attacks aimed at disrupting systems have been damaging for certain high profile websites like portals. Some studies have calculated that a recent attack caused damage worth several hundred million Euros, in addition to the intangible damage to reputation. Increasingly, companies rely on the availability of their websites for their business and those companies, which depend on it for "just in time" supplies are particularly vulnerable.

- **Execution of malicious software that modifies or destroys data.** The most well known type of malicious software is the virus. Infamous examples include the "I Love You", "Melissa" and "Kournikova" viruses. About 11 % of European users have caught a virus on their home personal computer (PC). There are other types of malicious software. Some damage the PC itself, whereas others use the PC to attack other networked components. Some programs (often called 'logic bombs') can lie dormant until triggered by some event such as a specific date, at which point they can cause major damage by altering or deleting data. Other programs appear to be benign, but when opened release a malicious attack (often called 'Trojan Horses'). Another variant is a program (often called a worm) that does not infect other programs as a virus, but instead creates copies of itself, which in turn create even more copies and eventually swamp the system.

[7] The definitions and text of the draft Framework Decision has since changed in a number of areas.

- **Interception of communications.** Malicious interception of communications compromises the confidentiality and integrity requirements of users. It is often called "sniffing".

- **Malicious misrepresentation.** Information systems offer new opportunities for misrepresentation and fraud. The taking of someone else's identity on the Internet, and using this for malicious purposes, is often called "spoofing".

The EU Council in response to September 11 have added to the above 'offences' two specific 'offences': serious attacks through illegal access to information systems, serious attacks through interference with information systems in *COM (2002) 173 Final*.

Article 3
Serious attacks through illegal access to Information Systems
Each Member State shall take the necessary measures to ensure that the intentional access, without right, to the whole or any part of an information system is punishable as a criminal offence where the conduct constitutes a serious attack.

Article 4
Serious attacks through interference with Information Systems
Each Member State shall take the necessary measures to ensure that the following intentional conduct, without right, is punishable as a criminal offence where it constitutes a serious attack:
(a) The serious hindering or interruption of the functioning of an information system by inputting or transmitting computer data.
(b) The serious hindering or interruption of the functioning of an information system by damaging, deleting, deteriorating, altering or suppressing computer data.
(c) The damaging, deletion, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system.

It is apparent that this perspective on the perceived threats adopts a rather different perspective than has been traditionally used in the UK. It is different in scope than the CMA-something that becomes immediately apparent when looking at the terminology used in the Framework Decision. For example:

Information System means computers and electronic communication networks, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance.
Electronic communications network means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, irrespective of the type of information conveyed or technology employed.
Computer means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data.
Computer data means any representation of facts, information or concepts which has been created or put into a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function.

3 COUNCIL OF EUROPE CONVENTION ON CYBER-CRIME

The Council of Europe recognised that digitalisation, convergence and continuing globalisation of computer networks offer huge benefits but also that computer networks and electronic information could also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks. The need for co-operation between States and industry in combating cyber-crime and the need to protect legitimate interests in the use and development of information technologies all informed the drafting of the final convention. It was also recognised that an effective fight against cyber-crime required increased, rapid and well-functioning international co-operation in criminal matters. The Convention pursued three aims:

- It laid down common definitions of certain criminal offences enabling national laws to be harmonised.
- It defined investigation and criminal prosecution methods appropriate to the computerised environment and enabling national criminal procedures to be brought more closely into line with each other.
- It defined ways and means of co-operating internationally against cyber crime, whether these are traditional or new.

The Convention was signed by the UK in November 2001. It will come into effect when there are at least 5 ratifications including at least 3 member States of the Council of Europe. To date (January 2003) there have been 2 ratifications, by Albania and Croatia. In ratifying a Convention, a State is allowed to avail itself of a number of reservations provided for in the text.

The extent to which UK laws are compatible with EU proposals and the Council of Europe Cyber Crime Convention remains a problem. Once the convention has been ratified, the UK will have to give effect to the Convention in domestic law.

The main substantive law provisions are:

Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent**,** or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.
Article 5 – System interference
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right measures dealing with the production, sale, procurement for use, import, distribution or otherwise making available of:
A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5, a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed for the purpose of committing any of the offences established in Articles 2 - 5

Computer-related offences:

Article 7 – Computer-related forgery
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:
Any input, alteration, deletion or suppression of computer data,
any interference with the functioning of a computer system,
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

Content-related offences:

Article 9 – Offences related to child pornography
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
Producing child pornography for the purpose of its distribution through a computer system,
offering or making available child pornography through a computer system;
distributing or transmitting child pornography through a computer system;
procuring child pornography through a computer system for oneself or for another;
possessing child pornography in a computer system or on a computer-data storage medium.

Offences related to infringements of copyright and related rights:

Article 10 – Offences related to infringements of copyright and related rights
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright.
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party…where such acts are committed wilfully, on a commercial scale and by means of a computer system.

4 CONCLUSION

There are perceived problems with the CMA in respect of the issues as mentioned above:

It is not simply a question of compatibility of terminology. Although, it may be useful to undertake an exercise of comparing the CMA and EU proposals ultimately it may not be possible to reconcile the differences between them.

The EU proposal discusses 'serious attacks' but note that the range of individuals, groups and States who may be involved is very wide ranging; the 'seriousness' of an attack may be the outcome of a technically brilliant 'computer nerd' because of the wide spread disruption to essential services that it causes. For example it is possible that hacking motivated by no more than simple mischief may nonetheless be extremely serious. By analogy with criminal damage (R v Abbot-a case involving the economic consequences of damaging GM crops) the wider economic consequences of a criminal act may not give rise to compensation under the criminal law, outside the immediate damage caused. Hacking under section 1 of the CMA is a summary only offence.

There is a problem in trying to reconcile the language used by the EU with UK law, this problem has been well recognised in European forums and discussions have been held in regarding the compatibility of UK criminal concepts when compared with the European continental system.

Whatever exercise is therefore undertaken as to compatibility may not be sufficient. It is likely that new primary legislation will be needed. The main areas of consideration are perceived to be:

The definition of "Information System" in ***Article 2*** is potentially wider than the term "computer" used in CMA. The phrase "information system" used by the EU can be contrasted with the CMA 1990 use of " computer". The CMA deliberately did not define what a computer was, nor did it provide a definition of a "computer system" nor of "computer data". But the CMA would not cover the range of networks that the EU proposal does. The CMA leaves detailed definition of the "computer", to the courts' to interpret.
Article 2 mentions "Without right" which is potentially confusing. Any definition would need to be consistent across Member States and therefore not dependent on domestic legislation. It does not appear to add anything to "unauthorised" as used in CMA.
This opportunity to tighten up the CMA definition of "unauthorised" in order that it may clearly cover authorised personnel (i.e. employees) whose authority has been limited for example given for a specific purpose and that specific purpose has been intentionally and deliberately exceed.

Article 3 is similar to section 1 CMA, but limits offences to attacks against protected systems. Section 1 CMA need not be limited to this specific requirement, since the section 1 offence encompasses this offence we would not need to change our legislation.

Article 4 is similar to section 3 CMA but goes beyond it. The term "impair" in the CMA is wider than "serious hindering or interruption" in ***Article 4(a),*** the word "serious" should be removed.
Article 4 lists ways in which the hindering or interruption may be achieved (a similar approach to CMA). This prescription provides certainty, but risks missing actions with the same effect, such as physically switching the power off.
"Inputting or transmitting" and "determination … suppressing or rendering inaccessible" all appear to add to the CMA use of "modification" and could be adopted by the CMA. This approach covers known Denial of Service attacks.

Articles 6 and 7 deal with penalties, the maximum sentence for section 1 CMA is presently 6 months imprisonment, this should be increased to at least 12 months imprisonment, which would allow section 1 to become an extraditable offence.

Consideration should be given to the penalty of the section 1 CMA offence to be increased to 5 years imprisonment this would bring the penalty in line with what already pertains to sections 2 and 3 CMA. Thus allowing sufficient sentencing powers for the potential serious nature of access to unauthorised data. This in turn would also mean Section 1 would then become an arrestable offence[8]. As an arrestable offence would have a power of search and seizure[9]. An additional benefit is that co-operation could be given to other countries in respect of search and seizure regarding offences committed outside the United Kingdom.[10] In certain circumstances an arrestable offence can become a serious arrestable offence, this gives the investigating officer additional powers under schedule 1 of PACE.[11]

Where an offence is triable only summarily, it cannot be an object of a criminal attempt under section 1 CMA; an increase in the sentence for this offence would solve this problem. Increasing the penalty of the section 1 offence would solve the time limit problem. Section 1 is a summary only offence and proceedings under this section may be brought within six months from the date on which evidence sufficient in the opinion of the prosecutor to institute proceedings came to his knowledge[12]. There is in any event an overall time limit of three years[13]. There could be a problem in deciding who is the prosecutor in a case, is it the police officer who investigated the crime? Or the Crown Prosecutor who has been asked to advise on the case?[14]

The tactics used by the police to investigate a more serious offence, if used to investigate a section 1 CMA summary only offence could be assessed as not being proportional (and therefore not compliant with Human Rights) for a summary only offence.[15]

In Scotland the CMA has only ever been used on a handful of occasions. Prosecutors have preferred to use charges at common law such as fraud or malicious mischief. These have a wide definition and carry a maximum sentence of life imprisonment. By using such charges prosecutors in Scotland can avoid many of the problems with the CMA highlighted above.

Obviously the European Convention provisions go much wider than the scope of the CMA. For example provisions dealing with fraud and pornography. Ensuring that UK law is compatible with the Convention requires that several statutes be considered.

As with the EU Framework Decision discussed in Part 3 some of the terminology used is not familiar to UK legislation and/or jurisprudence. For example 'without right'.

In addition there are provisions dealing evidential, procedural and jurisdictional issues that are outside the scope of the CMA. Inter-alia these include: Ancillary liability and sanctions *(Attempt and aiding or abetting; Corporate liability; Sanctions and measures*). Procedural law (*Common provisions;* Scope *of procedural provisions; Conditions and safeguards*). Expedited preservation of stored computer data *(e*xpedited *preservation of stored computer data; Expedited preservation and partial disclosure of traffic data*). Production orders. Search and seizure of stored computer data. Real-time collection of computer data (Interception of content data). Jurisdiction (International co-operation and general principles relating to international co-operation; Extradition; mutual assistance; Spontaneous information; Procedures pertaining to mutual assistance requests in the absence of applicable

[8] Section 24 PACE.
[9] Section 17 PACE.
[10] Section 7(1) Criminal justice (International Co-operation) Act 1990.
[11] Section 116 PACE.
[12] Section 11(2) CMA.
[13] Section 1(3) CMA.
[14] See R v Southwark Crown Court ex. P. Morgans, Queen's Bench Division DC 7 December 1998.
[15] A situation that a Computer Crime Unit had to deal with.

international agreements; Confidentiality and limitation on use). Expedited preservation of stored computer data. Expedited disclosure of preserved traffic data. Mutual assistance regarding accessing of stored computer data, mutual assistance regarding the real-time collection of traffic data. Mutual assistance regarding the interception of content data. Network and contact.

Again ensuring that UK law is compatible with the Convention requires that several statutes be considered. Each of these topics is complex (and often controversial) in its own right and merit separate consideration in further papers. It has been recognised by the government that the CMA and EU proposal, and later the CoE Convention text are not compatible and there will need to be a change to legislation.

We therefore consider that there are two ways forward for the CMA that are not mutually exclusive:

- An amendment to section 3 CMA 1990 is drafted.
- The CMA 1990 as a whole is amended in so far as is possible to meet (in due course) the EU Council Framework Decision discussed in Part 2 above and the EU Cyber Crime Convention as outlined in Part 3 above.

Any such amendments should incorporate the use of agreed terminology that is compatible (when possible) with these wider EU and Council of Europe initiatives. Because of the limited scope of the CMA consideration should be given as to whether the substantive criminal law in other related areas (for example fraud) also needs amendment and/or revision.

With reference to reform of the CMA this should also be considered with reference to procedural, evidential and jurisdictional issues that in turn will impact on enforcement of the substantive law. Further that such changes will impact more widely than Computer and High Tech Crime. Issues that should be considered as pressing in this regard include:

- Data protection issues.
- Information sharing between law enforcement agencies within the EU and globally and between public and private sectors.
- Surveillance and interception.
- Mutual legal assistance and reciprocity

Appendix A

Computer Misuse Act 1990

The CMA created three new offences in August 1990. Sections 1 and 2 of the CMA must be read in conjunction with section 17 of the CMA[16], they are the unauthorised access offence creating sections.

Section 1 of the CMA provides that:

(1) A person is guilty of an offence if –

He causes a computer to perform any function with intent to secure access to any program or data held in any computer,

The access he intends to secure is unauthorised; and

He knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at

Any particular program or data;

A program or data of any particular kind; or

A program or data held in any particular computer.

Section 17(2) CMA defines "secures access to any program or data" as:

Alters or erases the program or data;

Copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held,

Uses it; or

Has it output from the computer in which it is held (whether by having it displayed or in any other manner).

Section 17 (3) CMA states that a person uses a program if the function he causes the computer to perform causes the program to be executed; or is itself a function of the program. Almost any act involving use of the computer will be sufficient.

Attorney General's Reference (No.1 of 1991) [1993] Q.B 94 states that an offence is committed where the offender causes a computer to perform a function with intent to secure unauthorised access to any program or data held in the same computer. The words "any computer" in section 1 (1)(a) CMA is therefore not restricted to the situation where the offender uses one computer to secure unauthorised access to another computer.

The offence of unauthorised access requires proof of two mens rea elements:

There must be knowledge that the intended access was unauthorised; and
There must have been an intention to obtain information about a program or data held in a computer[17].

There has to be knowledge that the access is unauthorised on the part of the offender mere recklessness is not sufficient. This would cover not only hackers but also employees who exceed their authority[18].

[16] The interpretation section.
[17] Section 1 (2) CMA.

An offence contrary to section 1 CMA is a summary only offence, triable at the Magistrates' Court, a person is liable on conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both[19].

Proceedings for an offence under section 1 CMA may be brought within six months from the date on which evidence sufficient in the opinion of the prosecutor to institute proceedings came to his knowledge[20]. There is in any event an overall time limit of three years[21]. Section 1 CMA is not extraditable, as an offence has to be imprison able for 12 months or more to qualify under the extradition acts and treatise.

Section 2 CMA 1990

A person is guilty of an offence under section 2 of the CMA if he commits an offence under section 1 above ("the unauthorised access offence") with intent to commit or facilitate a further offence for which the sentence is fixed by law[22] e.g. murder; or one for which a person with no previous convictions might be sentenced to a period of five years imprisonment.

The section 2 CMA offence is triable either way and carries a maximum penalty of five years imprisonment if tried in the Crown Court. A person found not guilty of a section 2 or 3 CMA offence can be convicted of a section 1 offence[23].

Section 3 CMA 1990

(1) A person is guilty of an offence if –

He does any act which causes an unauthorised modification of the contents of any computer; and
At the time when he does the act he has the requisite intent and knowledge.

An offence under section 3 is committed when a person, acting with intent causes an unauthorised modification of the contents of any computer[24]. Section 17 CMA defines unauthorised modification as the alteration or erasure of any program or data, and encompasses the addition of any program or data[25]. A modification is unauthorised if the person causing it is not entitled to determine whether the modification should be made, and he does not have the consent of a person who is so entitled[26]. It is immaterial whether the modification or its effects are intended to be permanent or merely temporary[27].

The prosecution have also to prove under section 3 that the offender had the requisite intent[28] and knowledge[29]. This offence is triable either way and the maximum penalty in the Crown Court is the same as for section 2 CMA.

---

[18] See R v Bow Street Magistrates Court and Allison [1999] 3 WLR 620.
[19] Section 1 (3) CMA.
[20] Section 11 (2) CMA.
[21] Section 11 (3) CMA.
[22] Section 2(2)(a) CMA.
[23] Section 12 CMA.
[24] Section 3(1) CMA.
[25] Section 17 (7) CMA.
[26] Section 17 (8) CMA.
[27] Section 3 (5) CMA.
[28] Section 3(2) CMA states this is an intent to cause a modification of the contents of a computer by impairing the operation, preventing or hindering access to, or impairing the operation of any program or the reliability of data.
[29] Section 3(4) CMA defines requisite knowledge as "knowledge that any modification he intends to cause is unauthorised".

Appendix B

Proceedings at magistrates' courts and convictions at all courts under the Computer Misuse Act 1990, England and Wales 2001

Offence description		Proceeded against	Found guilty	Sentenced	Sentence breakdown: Absolute / conditional discharge	Fine	Community sentence	Immediate custody	Otherwise dealt with
Principal Offences [1]									
Unauthorised access to computer material - (Sec 1)		9	9	9	1	2	5	1	-
Unauthorised access with intent to commit or facilitate commission of further offences - (Sec 2)		4	3	3	-	-	1	2	-
Unauthorised modification of computer material - (Sec 3)		12	9	19	1	2	9	5	2
	Total	**25**	**21**	**31**	**2**	**4**	**15**	**8**	**2**
Non Principal Offences [1]									
Unauthorised access to computer material - (Sec 1)		23	12	12	1	-	4	-	7
Unauthorised access with intent to commit or facilitate commission of further offences - (Sec 2)		16	13	10	1	-	1	7	1
Unauthorised modification of computer material - (Sec 3)		19	23	9	-	-	9	-	-
	Total	**58**	**48**	**31**	**2**	**0**	**14**	**7**	**8**
All Offences									
Unauthorised access to computer material - (Sec 1)		32	21	21	2	2	9	1	7
Unauthorised access with intent to commit or facilitate commission of further offences - (Sec 2)		20	16	13	1	-	2	9	1
Unauthorised modification of computer material - (Sec 3)		31	32	28	1	2	18	5	2
	Total	**83**	**69**	**62**	**4**	**4**	**29**	**15**	**10**

(1) Principal offences are where an offence under the Computer Misuse Act carries the heaviest penalty to a charge against a person at a particular court appearance. Non-principal offences are any additional charges under the Computer Misuse Act against such persons together with subsidiary charges against other persons whose principal offence was not under the Computer Misuse Act.

Source: Offending and Criminal Justice Group (RDS), Home Office IOS: 524-02