2004 - All-Party Internet Group enquiry into the Computer Misuse Act 1990

This is JANET(UK)’s response to the All Party Internet Group's enquiry into the Computer Misuse Act 1990 [1].

JANET(UK) is the not-for-profit company that runs JANET, the UK’s education and research network, connecting universities, colleges and research establishments in the UK to each other and to the public Internet. JANET also provides inter-connection between schools networks in England, Scotland and Wales. JANET(UK) operates the JANET Computer Emergency Response Team (JANET-CERT), which responds to misuse of our own network and those of our customers. Our network is the target of both hacking and denial of service attacks, so we are concerned that UK legislation is able to prosecute such activities effectively. Our customer organisations also find it useful to have a clear statement in law that such activities are illegal so they can discourage students and others from attempting them.

We consider that the Computer Misuse Act 1990, as it has been interpreted by case law, covers most of the types of attack we experience. However one growing area of activity that may not be covered is Denial of Service attacks, where an attacker attempts to either crash or swamp a computer, organisation or network. Twenty-one of these attacks have been reported to us in the past three months; some of these were sufficiently serious to make even a large university’s network completely unusable for many hours. The aim of such an attack is to render a computer or network unable to perform its proper function, not to gain access to either computers or data. Although we are aware of legal arguments that such attacks are covered by the existing Act, these appear to depend on particular features of individual attacks. A clear statement in law that covers all deliberate and unauthorised interference with the proper function of an information system would be very welcome. Although we sympathise with the idea of punishing reckless use of computers and networks, as proposed in section 3A(2) of the Computer Misuse (Amendment) Bill published in 2002, we believe that this would be almost impossible to prosecute, as well as risking criminalising legitimate (if ill-advised) actions.

The Computer Misuse Act 1990 relies heavily on the concept of “unauthorised” actions, and the definition of this term in sections 17(5) and 17(8) of the Act has been criticised. The major problem, that a person’s authority to use a computer may only extend to some types of action and not others, appears to have been settled by case law. If a clearer statement were possible in legislation then this would be useful, however this must not be as restrictive as the use of “owner” in the Computer Misuse (Amendment) Bill.

The definitions of computer, data and program contained in the Act seem to have allowed sufficient judicial interpretation to cover the UK cases that have been reported. However we note that the European Framework Decision COM(2002)173 uses the term “information system”, and this wider term may now be more suitable for current and future technology. For

example where a Denial of Service attack achieves its purpose by simply filling a communications link to its capacity, it is not clear that this would constitute an attack on a “computer” although it would be an attack on an “information system”. Changes in terminology are likely to be necessary to make UK legislation comply with this Decision.

The large, and growing, number of attacks on information systems suggests that fear of punishment is not an effective deterrent. We believe that this is more likely to be due to the difficulty of prosecution than the severity of sentence that might result from a conviction. We would therefore expect to see greater benefits from improving the ability of the police to investigate and the courts to judge cases involving computers, networks and digital evidence than from simply increasing sentencing powers. However increasing the maximum sentence for the offence of unauthorised access (s.1 of the Act) would result in new powers becoming available to the police, in particular search and seizure (particularly important where fragile electronic evidence needs to be preserved) and international cooperation (most forms of computer misuse are international in scope), which would make investigation more effective. These side effects argue for increasing the maximum sentence for the unauthorised access offence.

Summary of Principal Recommendations

We believe that the law needs a clear statement that deliberate and unauthorised interference with information systems is unlawful.

We believe that the ability of the police to investigate crimes against computers, and hence the effectiveness of the law as a deterrent, would be improved by the additional powers that would become available if the maximum penalty for the crime of unauthorised access to a computer were to be increased.

Links
[1] http://www.apcomms.org.uk/apig/archive/activities-2004/computer-misuse-inquiry.html