Categorising cybercrime and cybercriminals: The problem and potential approaches

S.M.Furnell

Network Research Group,
Department of Communication and Electronic Engineering,
University of Plymouth,
Plymouth, United Kingdom.

sfurnell@plymouth.ac.uk

ABSTRACT

Cybercrime is now recognised as a major international problem, with continual increases in incidents of hacking, viruses, and other forms of abuse having been reported in recent years. However, although many people may recognise cybercrime-related terminology, agreeing and defining what they actually mean can prove to be somewhat difficult. As a result, alternative classifications have emerged from a range of authoritative sources, which are similar in some respects, but markedly different in others. This paper considers the difficulty associated with categorising cybercrime, and identifies that a harmonised nomenclature would be beneficial to individuals and organisations concerned with combating the problem, as well as to those concerned with reporting the issue to the general public. The discussion presents a variety of different top-level classifications of cybercrime, each of which has been utilised in practice by authoritative sources in the field. The need for further sub classification is then illustrated by examining the specific issue of hacking, which reveals that numerous types and motivations can be identified, and that the simple, yet frequently used, label of 'hacker' is consequently inappropriate to convey any real impression of the activities in many cases.

Keywords: Cybercrime, Hackers, Security.

INTRODUCTION

Cybercrime is now a major international issue, the effects of which have been felt in some way be the majority of the developed world. As networked computer systems have grown and matured, so too has the nature of crime and abuse within the environment. In the earlier days of computing, abuse was largely restricted to fraud and theft related activities, which simply represented the extension of traditional crimes into the electronic environment. However, as time has moved on, new and more advanced forms of abuse have emerged (e.g. computer viruses), which often appear not so much a means to an end, but an objective in themselves.

Recent survey results have revealed the increasing scale of the cybercrime problem. For example, the 2001 CSI/FBI Computer Crime and Security Survey reports financial losses totalling almost $378 million from 186 respondents, whereas the previous year had witnessed only $265.6 million from 249 respondents (CSI 2001). The 2001 survey also revealed that 85% of the 534 respondents had detected some form of security breach in the preceding twelve months. In view of such findings it is little wonder that many governments and law enforcement bodies around the world are increasing their efforts to address and control the cybercrime issue. In Europe, for example, the recognition of the growing problem and the need for a harmonised approach has prompted the drafting of a European Convention on Cybercrime (CoE 2000). However, whilst the general problem has been recognised, it has also been demonstrated that there are many different ways in which the underlying issues can be interpreted. This paper seeks to expose the significant variety that exists in cybercrime classification schemes, highlighting that this may represent a problem when attempting to make cross-comparisons between different assessments of the issue.

CATEGORISATIONS OF CYBERCRIME

At the most basic level, cybercrime can simply be interpreted as types of crime involving the use of computers. However, this is obviously a very broad description and to examine the issue more precisely it is useful to consider previous interpretations of computer crime and abuse that have been offered by some authoritative sources.

Parker (1998) distinguishes between the concepts of computer crime and cybercrime, and offers the following definitions:

Computer crime: A crime in which the perpetrator uses special knowledge about computer technology.

Cybercrime: A crime in which the perpetrator uses special knowledge of cyberspace.

Although perfectly acceptable as far as they go, these definitions are still rather too vague to enable the various dimensions of the problem to be appreciated. It is, therefore, appropriate to consider some other sources in an attempt to add some more specific definition.

Crime / abuse	**Description**
Fraud	• for private gain or benefit: – altering input in an unauthorised way; – destroying / suppressing / misappropriating computer output; – altering computerised data; – alteration or misuse of programs (excluding virus infections.
Theft	• of data; • of software.
Use of unlicensed software	• using illicit copies of software.
Private work	• unauthorised use of the organisation's computing facilities for private gain or benefit.
Misuse of personal data	• unofficial 'browsing' through computer records and breaches of data protection legislation.
Hacking	• deliberately gaining unauthorised access to a computer system, usually through the use of communication facilities.
Sabotage	• interfering with the computer process by causing deliberate damage to the processing cycle or to equipment.
Introducing pornographic material	• Introducing pornographic material, for example, by downloading from the Internet.
Virus	• distributing a program with the intention of corrupting a computer process.

Table 1 : Computer crime and abuse categories from UK Audit Commission (1998)

Over the last twenty years, the UK Audit Commission has conducted a series of surveys to determine the extent of the computer crime and abuse problem in both the UK public and private sectors. Looking at the issues encompassed by the surveys, it can be seen that, over the years, the recognised range of crimes has broadened. For example, in the 1981 survey the only categories were fraud and theft. However, by the time of the most recent survey in 1998, the range had more than quadrupled to encompass a variety of other problems. The full range of categories, along with the Audit Commission's own definitions of them, are presented in Table 1 (Audit Commission 1998).

Looking at the Audit Commission categories more closely, it is possible to draw a distinction between those crimes that are computer-assisted and those that are computer-focused, as defined below.

- **Computer-assisted crimes**. Cases in which the computer is used in an supporting capacity, but the underlying crime or offence either predates the emergence of computers or could be committed without them.

- **Computer-focused crimes**. Cases in which the category of crime has emerged as a direct result of computer technology and there is no direct parallel in other sectors.

Using these classes, it is clear that the Audit Commission headings of fraud, theft, unauthorised private work, misuse of personal data, sabotage and pornography all fall into the computer-assisted category. Meanwhile, hacking and viruses are definite by-products of the IT age and are, therefore, computer-focused. Problems of hacking and viruses clearly fall within this category. Categorising the use of illicit software is a debatable point, as it clearly would not be feasible without a computer. However, the underlying nature of the offence is a breach of copyright – something that frequently occurs in other domains such as music and publishing. As such, for the purposes of this discussion, it will be considered to fall into the computer-assisted class.

A diagrammatic representation of the different categories of cybercrime is presented in Figure 1. The dark shaded boxes denote computer-focused crimes, whereas the lighter ones represent the computer-assisted variety (the unshaded boxes are used for the higher level categorisations, within which both computer-assisted and computer-focused crimes will exist). The classifications in the table are not exhaustive and represent merely one way of thinking about the issues. For example, they could alternatively be grouped according to their resulting impacts (financial loss, destruction of data etc.) rather than the methods involved.

It can be seen that some further levels of detail have been added over and above the Audit Commission categories. For example, the issue of misuse of personal data has been broadened under the more general heading of invasion of privacy, and placed alongside the issues of harassment and identity theft – both of which can be effected through the online medium. Harassment may occur against organisations or against specific people – in the later case it may sometimes be referred to as 'cyber-stalking'. Equally, identity theft may be applied at both levels and, when targeted against an organisation, may be referred to as 'cyber-squatting'.

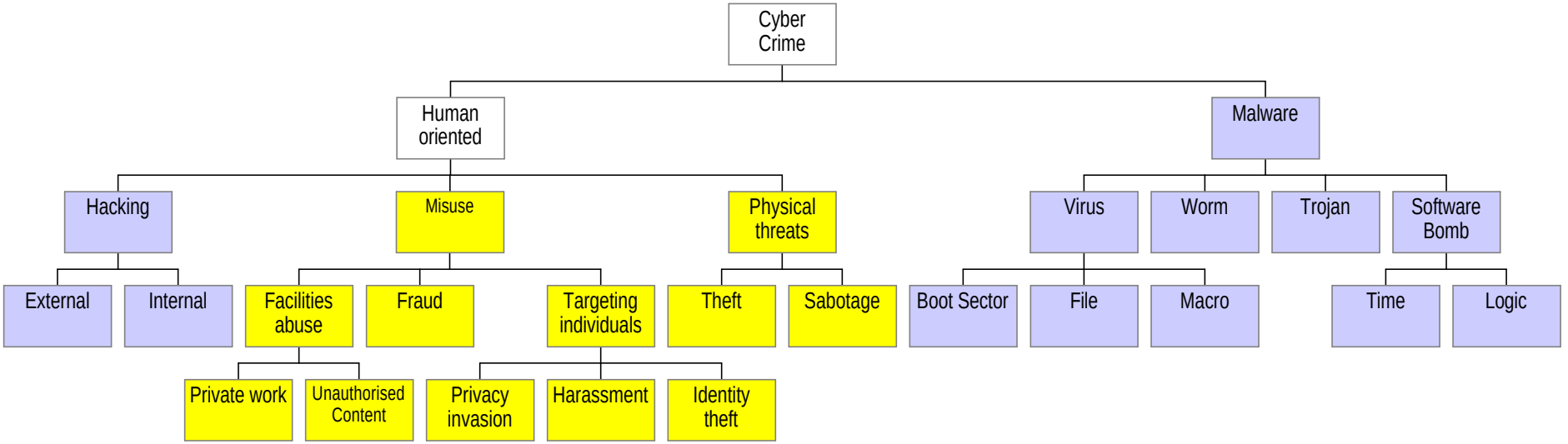

Figure 1 : Cybercrime categorisation

An alternative set of computer crime categories is provided by the FBI's National Computer Crime Squad (Fraser 1996), as listed below:

- Intrusions of the Public Switched Network (the telephone company)
- Major computer network intrusions
- Network integrity violations
- Privacy violations
- Industrial espionage
- Pirated computer software
- Other crimes where the computer is a major factor in committing the criminal offence

It can be observed that, in this case, hacking and viruses (the computer crimes with probably the highest level of media and public recognition) are not explicitly named. They are, however, the means by which a number of the categories could be realised.

To offer another, and final, view on the issue, the thirteen classifications used by the Computer Security Institute (CSI), as the basis for their 2001 Computer Crime and Security Survey, conducted in collaboration with the FBI, were as follows (CSI 2001):

- Theft of proprietary information
- Sabotage of data or networks
- Telecom eavesdropping
- System penetration by outsider
- Insider abuse of net access
- Financial fraud
- Denial of service
- Spoofing
- Virus
- Unauthorized insider access
- Telecom fraud
- Active wiretapping
- Laptop theft

It can be seen that in many cases, the descriptions refer to much more specific types of incident (e.g. denial of service, laptop theft), while others categories (such as virus) are very generic by comparison and could easily be subdivided further. At the same time, other classes of crime that were identified by the previous classifications (e.g. use of unlicensed or pirated software), do not appear to be encompassed by the CSI's headings.

The classifications presented here are by no means exhaustive and various other sources can be found that present further alternative versions. However, what should already be apparent from this discussion is that the general issue of cybercrime can be interpreted in many different ways. Although from one perspective this is not a problem, in the sense that each of the different organisations above are attempting to add value by making their own specific interpretations of a general problem, it can potentially become confusing for those wishing to more accurately understand or report cybercrime incidents. If everyone takes a different view of the problem, then it is more difficult to draw direct comparisons between different survey results and other such incident reports. This, in turn, makes it harder to get a full picture of the problem on an international level and make harmonised assessments of the scale.

CATEGORISATIONS OF HACKERS

Having looked at how the general issue of cybercrime can be decomposed into a variety of alternative first level groupings, it is also appropriate to consider how these sub-headings can, in turn, be further subdivided. This section illustrates the point by considering the single issue of hacking. Figure 1 presented a simplified sub-classification of this point, splitting the problem into just 'internal' and 'external' categories. However, it is possible to consider the issue of hacking in considerably more detail than this, which at the same time serves to illustrate that the classification problem continues at lower levels.

The definition of the term 'hacker' has changed considerably over the last 30 years. In the 1960s, hackers were the dedicated software and hardware gurus, and the term largely referred to persons capable of implementing elegant, technically advanced solutions to technologically complex problems. In the new Millennium, the moniker is more commonly used to refer to persons who gain unauthorised access to systems and data. At the extreme are a subset (often distinguished by the term 'crackers') that perform openly malicious actions upon the systems they enter, such as deleting files, modifying data and stealing information. The media is largely credited with misusing the term 'hacker' and an explicit distinction between hackers and crackers is maintained in certain writings. However, to argue that it is just the media that misuses the term is itself misleading – indeed, it is debatable whether this interpretation should be considered misuse at all. The nature of the computing industry has now changed and the commonly accepted meaning of the word 'hacker' (in an IT context) can be illustrated by considering dictionary definitions from recent years:

- "A computer fanatic, esp. one who through a personal computer breaks into the computer system of a company, government, etc." - Collins English Dictionary (3rd Edition), 1994.

- "A person who uses computers to gain unauthorized access to data" - The New Oxford Dictionary of English, 1998.

- "A skilled and enthusiastic computer operator, *esp* an amateur; an operator who uses his or her skill to break into commercial or government computer or other electronic systems" - The Chambers Dictionary, 1998.

It can be seen that specific emphasis is placed upon the issues of unauthorised access and breaking into systems. As such, for the public at large, the act of hacking is generally synonymous with these factors. In fact, the nature of the wording in some cases serves to imply that if an individual uses a computer for a hobby, but does not engage in unauthorised access, then they do not meet the definition of a true hacker. Clearly, these definitions are not compatible with the viewpoint of first-generation hackers, but they nonetheless seem to represent the generally accepted interpretation in modern society.

Whatever your preference, the use of a term such as hacker or cracker is still sometimes too vague. It is analogous to the use of a simple label such as 'criminal' to refer to a lawbreaker – the label alone is not very informative and there are a number of sub-categories that can be used to enable a more specific classification. Unfortunately, there is no overall set of hacker sub-groups that is regarded as definitive. There are, however, numerous terms that can be used to provide more specific focus and meaning. For example, a fairly high-level distinction can be made using the terms Black Hat and White Hat hackers. The former refers to the majority of hackers – those intruding into systems in an unauthorised, and frequently malicious, manner (to add yet another term, these may also be referred to as 'dark-side' hackers). White Hats, by contrast, are 'ethical' hackers, working for the good of system security. So, in a sense, these groupings can be considered to represent the same basic distinctions as the hacker and cracker labels defined earlier. It should also be noted that another term, Grey Hat, is used to refer to individuals who fall somewhere in between these two camps – those whose motives are unclear or may be prone to change.

In order to further illustrate the lack of a clear-cut black and white, good and bad distinction, the paragraphs below present some other names that are frequently ascribed to members of the hacker community (it should be noted that even this still does not purport to provide an exhaustive list).

- **Cyberterrorists.** Terrorists who employ hacker-type techniques to threaten or attack against systems, networks, and/or data. As with other forms of terrorism, cyberterrorist activities are conducted in the name of a particular political or social agenda. The underlying objective will typically be to intimidate or coerce another party (e.g. a government).

- **Cyber warriors.** Persons employing hacking techniques in order to attack computer systems that support vital infrastructure, such as emergency services, financial transactions, transportation and communications. This essentially relates to the application of hacking in military and warfare contexts.

- **Hacktivists.** Hackers who break into computer systems in order to promote or further an activist agenda. Incidents such as the defacement of web sites are very often linked to these individuals.

- **Malware writers.** Not strictly a classification of hacker – but often considered alongside them – these individuals are responsible for creating malware programs such as viruses, worms and Trojan Horses.

- **Phreakers.** Individuals who specifically focus upon hacking telephone networks and related technologies. Their objectives may range from simple exploration of the infrastructure to actually manipulating elements of it (e.g. to enable free phone calls to be made).

- **Samurai.** Individuals who are hired to conduct legal cracking jobs, penetrating corporate computer systems for legitimate reasons. Such hackers may also be termed **Sneakers**.

- **Script kiddies.** Individuals with fairly limited hacking skills who rely upon scripts and programs written by other, more competent, hackers. Hackers of this type typically cause mischief and malicious damage and are generally viewed with scorn by more accomplished members of the hacking community. Such individuals may also be referred to as **Packet Monkeys**.

- **Warez d00dz.** A sub-class of crackers, who obtain and distribute illegal copies of copyrighted software (after firstly breaking any copy protection mechanisms if appropriate). The spelling used is representative of a common form of hacker slang – in this case the two words, when written properly, are 'Wares Dudes'. More commonly, these individuals are known as **Software Pirates**.

From the above, it quickly becomes clear that the issue of hacking is as riddled with alternative classifications as the top-level issue of cybercrime. At the same time, the definitions have shown that many of the headings are not simply alternative names for the same thing – there is actually some difference between the different types of hacker. As such, saying that an individual is a hacker is really just as generic as saying that someone is a cybercriminal – it does not give enough definition. In the case of hackers, the difference essentially comes down to the motivations behind their actions. To illustrate this, a classification of hacker types against a variety of potential motivations is given in Table 2. Note that the column relating to 'Old School' hackers makes reference to the original hackers of the 50s and 60s, and those who share their values today. The intention is not to cast them as cybercriminals, but to enable a contrast between their motivations and the other groups that are often classed under the generic label of 'hacker'. In each case, the most likely motivator for the class of hacker is also indicated by the emphasized tick mark.

	Cyber-terrorists	Cyber Warriors	Hacktivist	Malware writers	Old School	Phreakers	Samurai	Script Kiddies	Warez d00dz
Challenge				✓	✓	✓	✓		✓
Ego				✓	✓	✓		✓	✓
Espionage		✓		✓					
Ideology	✓	✓	✓		✓				✓
Mischief				✓		✓		✓	
Money		✓		✓		✓	✓		✓
Revenge	✓		✓	✓				✓	

Table 2 : Hackers and their motivations

As the table suggests, a single hacker will not necessarily have a single motivation that drives his or her actions. In this sense, hacking skills can be regarded as generic – able to be applied as appropriate to the needs of a hacker at a particular time. It can also be observed that some motivations may apply to different groups in different ways. For example, the motivation of 'money' is indicated as applying to Phreakers, Samurai, Warez d00dz, malware writers and Cyber Warriors. For Phreakers, this motivation is in the sense of being able to avoid paying for calls. Samurai and Cyber Warriors are both being paid to do a job. Warez d00dz may be in the business of selling on their pirated offerings. Finally, some malware writers, as we will see later, may distribute their creations in order to support some form of money-making scam.

The above discussion illustrates that, as with the top-level classifications of cybercrime, the issue of hacking can be interpreted in many different ways. In many cases when reading information about hackers, it is essential to be sure that you are attuned to the correct terminology. Many sources, particularly media reports, utilise the different labels quite loosely, happily interchanging them in many cases. By contrast, other writers, demanding a greater degree of specificity, argue passionately for the correct distinctions to be maintained. This section has not sought to resolve the problem – merely to illustrate that the label of 'hacker' can be further decomposed, and that, in the context of discussing and analysing cybercrime, it is useful to do so in order to appreciate that different motivations may be at work. A more comprehensive discussion of the issue is provided in Furnell (2001).

CONCLUSIONS

The discussion has shown that cybercrime is not a straightforward concept to define. Whilst all of the classifications are appropriate when considered in isolation, attempting to compare and contrast them immediately reveals inconsistency, overlaps and omissions. As a result, without a clear and standardised nomenclature, the cybercrime issue risks being clouded by misunderstanding.

Of the top-level categorisations presented in this paper, the author considers that the UK Audit Commission's interpretation is the most straightforward – with fewer obvious overlaps between the different categories identified. Having said this, however, the categorisation could still be usefully decomposed into more specific levels of detail – particularly in relation to classifications such as hacking and viruses.

The discussion of hackers has sought to further demonstrate the ease with which different interpretations can be placed upon what some people would prefer to neatly describe as a single issue. Although it removes the simplicity, it is appropriate to make such further distinctions in many circumstances, in order to remove ambiguity and reduce misunderstandings. The desirability of at least distinguishing between hackers and crackers provides an illustration of this, as does the frequent misapplication of the term virus, which is often incorrectly used as a catchall name for other forms of malware such as worms and Trojan Horses.

If a suitably standardised set of names can be devised then it can be used as the basis for improving education and raising awareness in relation to cybercrime at several levels. This could include the security community that seeks to protect systems against cybercrime, as well as the governments and law enforcement bodies that attempt to control the problem, and the media that reports it to the public at large.

REFERENCES

Audit Commission. (1998). *Ghost in the Machine – An Analysis of IT Fraud and Abuse*. The Audit Commission, United Kingdom.

CoE. (2000). *Draft Convention on Cyber-Crime (Draft No 19)*, Council of Europe, PC-CY (2000) Draft No 19. Strasbourg 25 April 2000.

CSI. (2001). '2001 CSI/FBI Computer Crime and Security Survey', *Computer Security Issues & Trends*, vol. VII, no. 1. Computer Security Institute. Spring 2001.

Fraser, B.T. (1996). 'Definition of 'Computer Crime'', Computer Crime Research Resources, http://mailer.fsu.edu/~btf1553/ccrr/welcome.htm#definition

Furnell, S.M. (2001). *Cybercrime: Vandalising the Information Society*. Addison-Wesley. ISBN 0201721597

Parker, D.B. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*. John Wiley & Sons Inc., New York.