# Chapter 2
# Unauthorized Access Offences in Cyberworld

## 2.1 Emerging Threats: Expected Targets and Forms

Computer hacking is the accessing of a computer system without the express or implied permission of the owner of that computer system (Bainbridge 2004, p. 381). A person who engages in this activity is known as a computer hacker and may simply be motivated by the mere thrill of being able to outwit the security systems contained in a computer. Hackers may gain access remotely, using a computer in his own home or office connected to a telecommunications network (Ibid).

Hacking can be thought of as a form of mental challenge, not unlike solving a cross word puzzle, and the vast majority of hacking activities have been relatively harmless. Sometimes, the hacker has left a message publicizing his feat, reflecting the popular image of a hacker as a young enthusiast who is fascinated by computers and who likes to gain access to secure computer systems to prove his skills to himself or his peers (Ibid).

Computers can be the target of a criminal activity, a storage place for data about a criminal activity and/or the actual tool used to commit a crime (planning criminal activity). One of the most publicized crimes targeting computers involves unleashing a virus through email. A virus is a computer program that disrupts or destroys existing computer systems. A virus spreads rapidly around the world destroying computer files and costing companies and individuals millions in downtime (time when the computers or networks are shutdown). Most viruses are released by hackers as pranks. A hacker is someone who gains unauthorized access to a specific system. Sometimes hackers may target law enforcement or military computers and read or copy sensitive (secret or private) information. Some are concerned that terrorists will unleash viruses to cripple computer systems that control vital transportation networks.



M. Chawki et al., *Cybercrime, Digital Forensics and Jurisdiction*,
Studies in Computational Intelligence 593, DOI 10.1007/978-3-319-15150-2_2

Once the hacker has penetrated a computer system he might do one of several different things. He might read or copy highly confidential information; erase or modify information or programs stored in the computer systems; download programs or data, or he might simply add something, such as a message, boasting of his feat. He might also be tempted to steal money or direct the computer to have goods sent to him.

In days before computers, sensitive information was kept locked away in filing cabinets in locked rooms on the premises of the organization holding the data. This way the sensitive information was safe from being tampered with or copied.

By contrast, information stored on a computer that is linked to a telecommunication system is much more vulnerable. It is analogous to information stored in paper files kept in locked cabinets but left in a public place. It is just a matter of finding the right key to fit the cabinet; not only can a total stranger try the lock, but, often he can spend as long as he likes trying different keys with impunity until he finds one that works.

A recent example of hacking's dangerous effects can be seen in the various botnet conspiracies currently plaguing the country (Department of Justice 2010, Online). As background, "botnets" are "collections of software agents that run automatically" to commandeer massive numbers of computers to allow cybercriminals to conduct large-scale "malicious activity including spreading spam, stealing log-in credentials and personal information or distributing malware to others." (Pinguelo and Muller 2011, p. 132). In one small example, conspirators allegedly created a coded botnet program, which could be used to hack into and control another person's computer. Once transmitted, the program caused the infected computers to log onto a website and wait for commands, allowing the men to control and command the botnet.

With the botnet subject to their every whim, the men accessed, without permission, the user database of T35.net, a website which offered personal and business web-hosting services for thousands of users (Department of Justice 2010, Online). The database contained confidential user identifications and passwords, which the defendants downloaded. Soon thereafter, the men defaced the T35.net website and exposed the customers' user ids and passwords to the public (Ibid).

It is not only small companies that are vulnerable to botnet attacks, as in 2010, large corporations such as Google, Adobe, and several others were victimized by a targeted botnet attack called "Aurora." According to an industry insider, "the Aurora botnet was targeted against large international businesses with the goals of network infiltration, theft of business secrets and modification of critical systems data."

## 2.2 Criminal Statues

### *2.2.1 United States*

#### 2.2.1.1 The CFAA

The CFAA is a computer security statute aimed at protecting the computers operated by the federal government and banking institutions, and computers linked to the Internet. It creates criminal liability for "trespassing, threats, damage, espionage," and for government computers "being corruptly used as instruments of fraud."

#### 2.2.1.2 Access Device Fraud

Section 1029 outlaws the "production, use, possession, or trafficking of unauthorized or counterfeit access devices." In relation to Cybercrime, the DOJ asserts that the statute could be used to prosecute a cybercriminal who employs "phishing" emails to obtain victims' private passwords and financial account numbers, or where the cybercriminal deals in stolen bank account or credit card information. The penalties for this variety of fraud are severe, including civil forfeiture and prison terms ranging from a maximum of 10 or 15 years for first time offenders, with repeat offenders being subject to a potential 20 years jail sentence.

#### 2.2.1.3 Stored Wire and Electronic Communications and Transactional Records Access

This statute criminalizes the unauthorized access of email and voicemail. The felony version of the crime has five basic elements: (1) intentional access; (2) without or in excess of authorization; (3) access of a facility where an electronic communication service (ECS) was provided; (4) the defendant obtained, altered, or prevented authorized access to a wire or electronic communication while it was in "electronic storage;" and (5) the defendant acted "for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act…". For first-time offenders who lack the fifth "purpose" element, the maximum penalty is 1 year imprisonment and substantial fines, while repeat violators who lack the "purpose" element, or first-time offenders who commit the act with the "purpose" discussed above, face up to 5 years in prison and heavy fines. Repeat violations that run afoul of the improper purpose element expose the offender to a prison term of up to 10 years, coupled again with extensive fines.

#### 2.2.1.4 Wiretapping and Eavesdropping

In the United States, the use of wire, telephone, or television communication facilities for the purpose of executing a scheme to defraud or obtain money or property by false presences is a federal offence, even where the underlying fraudulent activity is strictly not a federal or state offence.[1] Such use must be proved to be in furtherance of the scheme and not merely incidental to it.

The wiretapping laws predate and hence were not designed to deal with the problem of unauthorized access to a computer, and whether they apply in a given case is inevitably somewhat arbitrary. In *US v Seidlitz* the use of telephone wires to copy computer software led to a wire fraud conviction and in *US v Rifkin* there was a conviction for fraudulent wire transfers. On the other hand in *US v Alston*, where the defendant used keys on a computer to alter personal credit files, thereby enabling unqualified persons to gain cars and other items on credit, the legislation was held not to apply. This is an example of the fortuitous application of existing criminal offences to a new problem, and it cannot be regarded as an appropriate solution to the question of unauthorized access to the computer.

The wiretap statutes current in many other jurisdictions refer expressly to the interception of oral communications or conversations and hence these statutes are inapplicable to the accessing of computers. The Italian Penal Code, for instance refers to communications "between persons", as does the German Penal Code.

In the key Canadian case of McLaughlin, this type of legislation was found to be inadequate and a case of unauthorized access to a computer. In early 1977, Michael McLaughlin made use of a computer owned and operated by the University of Alberta. The university's computer had about three hundred terminals located in and around the campus, connected to the central processing unit by coaxial cable and telephone lines. Mr. McLaughlin used one such terminal to use the computer's central processing unit without authorization.

Michael McLaughlin was charged with theft contrary to s.287(1)(b) of the Criminal Code for "fraudulently and without colour of right" using a "telecommunication facility".[2] Mr. McLaughlin was convicted of theft at trial. The trial judge considered that the central processing unit computer, the memory, the printers and the terminals constituted a telecommunications facility.

The Alberta Court of Appeal held that the accent of the computer facility was on computing and calculation and that the relay or communication aspect was only incidental, and hence allowed the appeal.

The Supreme Court of Canada agreed with the findings of the Alberta Court of Appeal that the university computer facility was not a "telecommunications facility" and that Mr. McLaughlin was therefore not guilty of theft under s.387(1)(b). Mr. Justice Estey, one of the panel of judges at the Supreme Court of Canada, invited Parliament to amend the Criminal Code at page 341 of the reported

---

[1] *US* v *Kelly 507* F Supp 495, 498 n6 (ED Pa 1981), *US v Gallant* 570 F Supp 303 (SDNY1983).

[2] (1979) 19 A.R. 368 (Alta. C.A.); (1980) 2 S.C.R. 331.

decision: "Had Parliament intended to associate penal consequences with the unauthorized use of a computer, it no doubt would have done so in a section of the Criminal Code or other penal statute in which the term which is now so permanently embedded in our language is employed".

#### 2.2.1.5 Pending Federal Legislation

In February 2010, the House of Representatives passed H.R. 4061, the Cybersecurity Enhancement Act of 2010 (Chabrow 2010, Online). The bill, which the Congressional Budget Office (CBO) estimated would cost $639 million from 2010 to 2014 and $320 million thereafter, would have, among other things, assisted the federal government's efforts in developing skilled personnel for its cybersecurity team, organized and prioritized the various aspects of the government's cybersecurity research and development, improved the shifting of cybersecurity technologies to the marketplace, and strengthened the role of the National Institute of Standards and Technology in developing and implementing cybersecurity public awareness and education programs to promote best practices (Ibid).

The Senate's counterpart cybersecurity legislation, S.773: Cybersecurity Act of 2010, was reported on by the Senate Committee on Commerce, Science, and Transportation in March 2010, which recommended that it be considered by the full Senate. The CBO estimates that the Senate bill would cost approximately $1.4 billion from 2011 to 2015. But, although congressional staffers made progress putting together a cybersecurity package that could pass the Senate, and despite the fact that Senate Majority Leader Reid emphasized passing a cybersecurity bill in 2010, industry opposition and partisan bickering stymied the passage of comprehensive reform by the 111th Congress (Bartz 2010, Online). Part of the reason for the delay may be that some members of congress had concerns relating to increased government control of the internet, as the Senate Bill gave the president the power to initiate contingency plans to ensure that vital federal or private services do not go offline in the event of a major cyberattack (Pearlman 2010, Online).

Similar concerns over presidential powers were seen in the opposition to S.3480: Protecting Cyberspace as a National Asset Act of 2010, the so-called "kill switch bill," which would have given the President broad emergency powers to protect critical digital infrastructure following a cyber-attack. Another reason for the failure of comprehensive cybersecurity reform in 2010 was that the White House did little to pressure Congress to move on the bill, in part because the political value of doing so would be minimal considering that cybersecurity receives such little attention from the average voter, and because the administration has been focused on improving the executive branch's readiness (Chabrow 2010, Online).

In 2011 the prospects for comprehensive reform are no better, as the looming presidential election and gridlock caused by a split Congress made one technology expert opine that "the chance of having a comprehensive anything in 2011 with this Congress is slim to none." (Gross 2011, Online).

### 2.2.2 United Kingdom

Section 1 of the Computer Misuse Act 1990 is aimed directly at hackers who gain access to computer programs or data without any further intention to carry out any further act. It says that 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, or to enable any such access to be secured;
- The access he intends to secure, or to enable to be secured is unauthorized; and
- He knows at the time when he causes the computer to perform the function that that is the case.

The intent does not have to be directed at any particular program or data, at programs or data of a particular kind, or at programs or data held in any particular computer.

A person guilty of an offence under this section shall be liable:

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months, or to a fine not exceeding the statutory maximum, or to both;
(b) on summary conviction in Scotland, to imprisonment for a term not exceeding 6 months, or to a fine not exceeding the statutory maximum, or to both;
(c) on conviction on indictment, to imprisonment for a term not exceeding 2 years, or to a fine, or to both

Section 17 of the Act contains definitions and other aids to interpretation but the Act does not define "computer", "program" or "data". Securing access is widely defined as causing a computer to perform any function, altering or erasing a program or data, copying or moving it to a different location in the storage medium in which it is held, using it or having output from the computer in which it is held. Access to a program includes access to a part of a program.

The offence is committed if the hacker simply intends to make access regardless of whether he/she succeeds but he/she must know, at the time, that the access is unauthorized. Careless or reckless access will not suffice. Because copying is within the meaning of securing access, potentially it can be an offence under section 1 to make a pirate copy of a computer program or other software or to download an unauthorized copy of a computer program.

#### 2.2.2.1 Authorised Access for an Unauthorised Purpose

An employee may have authorisation to use a computer system as a normal part of his duties to his employer. If the employee subsequently uses the system for an auauthorised use—for example, for his own purpose such as carrying out private work or retrieving information for other purposes unconnected with the employment—does

the access become unauthorised for the purposes of the Computer Misuse Act 1990? An example of this form of unauthorised use is given by the Audit Commission. A nurse at a hospital had authorisation to use the patient administration system but used it to search for medical details relating to friends and relatives. She then discussed these details with other members of her family. The nurse in question was not prosecuted under the Act, but given a written warning for this breach of patient confidentiality.

Where authorized access is used for an unauthorised purpose, is that access authorised? Two police officers had used the police national computer to gain access to details of motor cars which they wanted for private purposes unconnected with their duties as police officers. They were charged with the unauthorized access to computer material offence under section 1 of the Computer Misuse Act 1990 and convicted at Bow Street Magistrates' Court. However, their appeals to Southwark Crown Court were allowed and then confirmed by the Queen's Bench Divisional Court. In this case, the sole issue was whether the access was authorized. The divisional court held that it was, even though the purpose of the access itself was not authorized.

The court decided that as the police officers were, in fact, entitled to control access to the material within section 17(5) they were authorized to access the computer data even if this was for an unauthorized purpose. As part of their normal duties, the police officers were entitled to access such computer information. But being entitled to access computer material is not the same as being entitled to control access to such material. This is an important and crucial distinction which the court failed to make.

#### 2.2.2.2 Jurisdiction

The international character of some cybercrimes has caused concern about the possibility of criminals escaping prosecution because of jurisdictional issues. In 1985 an accused sent a telex from London intending to divert funds from New York to the accused's account in Geneva. It was held in the Court of Appeal that, had the attempt been successful, the theft would have taken place in New York and the English courts would not have had jurisdiction to try the perpetrator. To prevent this type of problem, the Computer Misuse Act contains complex provisions relating to jurisdiction and extradition in sections 4–9. All that is required is a link with the home country—England and Wales, Scotland or Northern Ireland (as appropriate). That is, the offence must either originate in the home country or be directed to a computer within it: for example, a person from within England attempting to carry out a computer fraud in Sweden, or a person in Italy attempting to hack into a computer located in London.

A final requirement is that of double criminality; that is, if the person operates from within any of the home countries, yet is intending to commit a further offence

under section 2 in a different country, that offence is indeed a criminal offence in that other country as well as in the home country. Of course, in most cases this will not present many problems—most countries recognize theft and fraud.

## 2.3 Other Offences Associated with Hacking

In this section we will some other offences which are associated with hacking.

### *2.3.1 Unauthorized Modification of Computer Programs or Data*

In the United Kingdom, under s3 (1) of the Computer Misuse Act 1990 a person is guilty of an offence if:

(a) he undertakes any act which causes an unauthorised modification of the contents of any computer; and
(b) at the time when he undertakes the act he has the requisite intent and the requisite knowledge.

"Authorization" was applied in a similar manner as it was to the offence of unauthorized access to computer material under s1 of the Computer Misuse Act 1990. Section 17 of the 1990 Act, which dealt with interpretation, gave a thorough, but at the same time broad, definition of modification, chiefly aimed at computer viruses and other forms of software which can cause severe damage to computer systems. In summary, modification is the alteration, erasure or addition of any program or data to the contents of a computer. The addition of a program or data includes the addition of computer viruses and other malicious software. The requisite intent under s3(1)(b) of the Act is defined under s3(2) as an intent to cause a modification of the contents of any computer, and by-so-doing:

(a) impairing the operation of any computer;
(b) preventing or hindering access to any program or data held in any computer; or
(c) impairing the operation of any such program or the reliability of any such data.

The intent need not be directed at any particular computer, program or data, or at programs or data or modifications of a particular kind, or at a particular modification. All that is required is knowledge that the intended modification is unauthorized.

#### 2.3.1.1 Unsolicited Emails

Since adding data to a computer falls within the definition of modification, the question arises as to whether a person who adds data to, for example, a computer disk, without authorization, has the requisite intent. In 2006 the defendant was dismissed from his employment and subsequently sent several hundred thousand emails to his former employer's computer system, which purportedly came from the company's HR manager. Charges were brought under s3 of the Computer Misuse Act 1990 for making an unauthorized modification to the contents of a computer. In the first instance, the judge held that the emails were authorized as the employer's computer system was set up to receive email. It was also held that s3 was designed to prevent the sending of material such as computer viruses. On appeal, the High Court concurred that a person who sets up a computer to receive emails is giving consent to emails being sent to that computer. But the consent does not extend to emails sent not for communication purposes but to disrupt the system.

#### 2.3.1.2 Scope of the Offence

The scope of the s3 offence is fairly broad, but also well-defined, and covers viruses, Trojans, time-bombs (a computer virus which is triggered by a specific date) and logic bombs (a program which will trigger a malicious function if certain conditions are met). A number of successful prosecutions have been brought under s3 for various types of conduct. A freelance typesetter, for example, altered a client's computer with the consequence that the client was denied access, and was consequently convicted under s3.

#### 2.3.1.3 The New s3 Offence as Introduced by the Police and Justice Act 2006

The Police and Justice Act 2006 has introduced a new s3 offence with the new title of "unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer, etc." The relevant provisions came into force on 1 October 2008. The offence is now committed by a person who undertakes an unauthorized act relating to a computer, knowing that the act is unauthorized, and intending the act to cause, or being reckless as to whether the act will cause, one of the following:

(a) the impairment of the operation of any computer;
(b) the prevention or hindering of access to any program or data held in any computer;
(c) the impairment of the operation of any such program or the reliability of any such data; or
(d) the enablement of any of the things mentioned in paragraphs (a)–(c) above.

As before, the intent or the recklessness need not be directed at any particular computer, program or data, or at programs of a particular kind. The new s3 also has more severe penalties for conviction, the maximum being 10 years imprisonment for a conviction on indictment.

### 2.3.2 Computer Viruses

A computer virus is a self-replicating program which spreads throughout a computer system, attaching copies of itself to ordinary programs. Often, by the time the virus is detected, many back-up disks also will have been infected. Rumours abound to the effect that viruses are far more likely to be on disks containing pirated software (Bainbridge 2004 p. 399).

There are literally, thousands of viruses and strains of viruses; some are relatively innocuous, like the Italian virus which causes a bouncing ball to appear on screen, but others are more pernicious and may completely corrupt a hard disk. The "AIDS" disk mentioned earlier was distributed as part of a blackmail scheme to over 30,000 organisations world-wide. Other recent viruses causing havoc and considerable expense, estimated to run into billions of dollars world-wide, were the "I Love You", SirCam and Melissa viruses (Ibid).

Obviously, viruses are going to remain a threat in the future but persons responsible for deliberately introducing them into a computer system are clearly guilty of an offence under section 3 of the Computer Misuse Act 1990. This is so even if the perpetrator does not personally carry out the act causing the infection. Section 3 states that the person is guilty if he undertakes any act which causes unauthorised modification. This includes distributing infected disks (Ibid).

Publishing details of how to write computer viruses could fall within the law of incitement; that is, the person publishing the details could be inciting others to commit a section 3 offence. However, there must be an intention on the part of the inciter to bring out the criminal consequences and this may be difficult to prove. In May 1995, an unemployed man who called himself the "Black Baron" became the first person to be convicted of incitement in respect of computer viruses. He was also convicted of 11 charges under the Computer Misuse Act 1990 and the judge warned him to expect a custodial sentence.

There is also a possibility of a charge as an accomplice but, again, intention must be proved. Obvious doubts about the applicability of the law of incitement and accomplices were confirmed by police fears concerning the then imminent publication of a book revealing virus techniques in 1992. The same difficulties apply in regard to access providers on the internet, through individuals responsible for posting details of how to write and spread viruses could be liable to prosecution (Ibid).

Bearing in mind the international nature of the internet, jurisdiction and extradition will be problematic in many cases.

## 2.4 Summary

Although transnational crime predates the digital age, digital technology has certainly facilitated it, and has posed new challenges for prosecutors. It is safe to assume that cross-border offences are more common today than in years past, and the need for cooperation between criminal justice agencies in different countries is greater than ever before. The traditional mechanisms of international cooperation, including mutual assistance, and other formalities with roots in the 19th century and earlier, are ill-suited to an era where offences can be committed from across the world at the speed of light.

## References

D. Bainbridge, *An Introduction to Computer Law* (Longman, New York, 2004)
D. Bartz, Analysis: cybersecurity bill on list for passage this year (2010), http://www.reuters.com/article/idUSTRE6885MF20100909. Accessed 14 July 2011
E. Chabrow, House passes cybersecurity enhancement act (2010), www.govinfosecurity.com/articles.php?art_id=2166. Accessed 14 July 2011
Department of Justice, Another pleads guilty in botnet hacking conspiracy (2010), http://www.cybercrime.gov/smithPlea2.pdf. Accessed 13 July 2011
G. Gross, Congress may be able to tackles tech issues in 2011 (2011), http://www.pcworld.com. Accessed 14 July 2011
A. Pearlman, Federal cybersecurity programs (2010), http://www.fed-soc.org. Accessed 14 July 2011
F. Pinguelo, B. Muller, Virtual crimes, real damages. VJLT **16**(1) (2011)

http://www.springer.com/978-3-319-15149-6

Cybercrime, Digital Forensics and Jurisdiction
Chawki, M.; Darwish, A.; Khan, M.A.; Tyagi, S.
2015, XVIII, 145 p., Hardcover
ISBN: 978-3-319-15149-6