Chapter 1
Cybercrime: Introduction, Motivation and Methods

1.1 Introduction

Advancements in modern technology have helped countries to develop and expand their communication networks, enabling faster and easier networking and information exchange. In less than two decades, the internet has grown from a curiosity to an essential element of modern life for millions. In addition to the socio-economic benefits, there is no doubt about computer technology and the internet that enhances the capabilities of human interaction. But somewhere the growth of global connectivity is inherent to cybercrime. Table 1.1 illustrates some interesting facts about the usage of ICT.

1.1.1 Definition

Computer-related crime or "cybercrime" or "e-crime" or "digital technology crime" is a long-established phenomenon, but the growth of global connectivity is inseparably tied to the development of contemporary cybercrime. Any criminal activity that involves a computer either as an instrument, target or a means for perpetuating further crimes comes within the ambit of cybercrime. A generalized definition of cybercrime may be "*unlawful acts wherein the computer is either a tool or target or both*".

The proliferation of digital technology and the convergence of computing and communication devices have transformed the way in which we socialise and do business. While overwhelmingly positive, there has also been a dark side to these developments. Crime follows opportunity; virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes. "Cybercrime" has been used to describe a wide range of offences, including offences against computer data and systems (such as "hacking"), computer-related forgery

M. Chawki et al., *Cybercrime, Digital Forensics and Jurisdiction*,
Studies in Computational Intelligence 593, DOI 10.1007/978-3-319-15150-2_1

Table 1.1 Global connectivity scenario

In 2014, more than one third of the world's total population had access to the internet
Over 60 % of all internet users are in developing countries, with 45 % of all internet users below the age of 25 years
It is estimated that mobile broadband subscriptions will approach 70 % of the world's total population by 2017
In the future hyper-connected society, it is hard to imagine a 'computer crime', and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity
There are nearly 2 billion internet users and over 5 billion mobile phone connections worldwide
Every day, 294 billion emails and 5 billion phone messages are exchanged

and fraud (such as "phishing"), content offences (such as disseminating child pornography), and copyright offences (such as the dissemination of pirated content).

The magic of digital cameras and sharing photos on the Internet is exploited by child pornographers. The convenience of electronic banking and online sales provides fertile ground for fraud. Electronic communication such as email and SMS may be used to stalk and harass. The ease with which digital media may be shared has led to an explosion in copyright infringement. Our increasing dependence on computers and digital networks makes the technology itself a tempting target; either for the gaining of information or as a means of causing disruption and damage. The idea of a separate category of 'computer crime' arose at about the same time that computers became more mainstream.

Generally speaking, computers play four roles in crimes: They serve as objects, subjects, tools, and symbols (Parker 1998). Computers are the objects of crime when they are sabotaged or stolen. There are numerous cases of computers being shot, blown up, burned, beaten with blunt instruments, kicked, crushed and contaminated (Ibid). The damage may be intentional, as in the case of an irate taxpayer who shot a computer four times through the window of the local tax office; or unintentional, as in the case of a couple who engage in sexual intercourse while sitting on computer sabotage and destroy information, or at least make it unavailable. Computers play the role of subjects when they are the environment in which technologies commit crimes. Computer virus attacks fall into this category. When automated crimes take place, computers will be the subjects of attacks. The third role of computers in crime is as tools, enabling criminals to produce false information or plan and control crimes. Finally, computers are also used as symbols to deceive victims. In a $50 million securities-investment fraud case in Florida, a stock broker deceived his victims by falsely claiming that he possessed a giant computer and secret software to engage in high-profit arbitrage. In reality, the man had only a desktop computer that he used to print false investment statements. He deceived new investors by paying false profits to early investors with money invested by the new ones (Parker 1998).

In the United States, police departments are establishing computer crime units, and cybercrime makes up a large proportion of the offences investigated by these divisions. The National Cybercrime training Partnership (NCTP) encompasses local, state, and federal law enforcement agencies in the United States.[1] The International Association of Chiefs of Police (IACP) hosts an annual Law Enforcement Information Management training conference that focuses on IT security and cybercrime.[2] The European Union has created a body called the forum on Cybercrime, and a number of European states have signed the Council of Europe's Convention on Cybercrime treaty, which seeks to standardize European laws concerning cybercrime. From this perspective, each organization and policy maker has their own ideas of what cybercrime is and isn't. These definitions may vary considerably. To effectively discuss cybercrime in this part, however, we need a working definition. Toward that end, we start with a board, general definition, before moving towards a more specific one.

When speaking about cybercrime, we usually speak about two major categories of offence: in the first, a computer connected to a network is the target of the offence; this is the case of attacks on network confidentiality, integrity and/or availability.[3] The other category consists of traditional offences such as theft, fraud, and forgery which are committed with the assistance of/or by means of computers connected to a network, computer networks and related information and communications technology. Cybercrime ranges from computer fraud, theft and forgery to infringements of privacy, the propagation of harmful content, the falsification of prostitution, and organized crime. In many instances, specific pieces of legislation contain definitions of terms. However legislators don't always do a good job of defining terms (Shinder 2002, p. 6). Sometimes they don't define them at all, leaving it up to law enforcement agencies to guess, until the courts ultimately make a decision (Ibid). One of the biggest criticisms to the definition of computer crime conducted by the U.S Department of Justice (DOJ) is of its overly broad concept. The (DOJ) defines computer crime as "any violation of criminal law that involved the knowledge of computer technology for its perpetration, investigation, or prosecution". Under this definition, virtually any crime could be classified as a computer crime, simply because a detective searched a computer database as part of the investigation.

One of the factors that make a hard-and-fast definition of cybercrime difficult is the jurisdictional dilemma. Laws in different jurisdictions define terms differently, and it is important for law enforcement officers who investigate crimes, as well as network administrators who want to become involved in prosecuting cybercrime that are committed against networks, to become familiar with the applicable laws (Ibid).

---

[1] *See* NCTP http://www.nctp.org.

[2] Ibid.

[3] Ibid.

One of the major problems with adequately defining cybercrime is the lack of concrete statistical data on these offences. As the reporting of crime is voluntary, the figures are almost certainly much lower than the actual occurrence of networked-related crime.

In many cases, crimes that legislators would call cybercrimes are just the 'same old stuff', except that a computer network is somehow involved. The computer network gives criminals a new way to commit existing crimes. Statutes that prohibit these acts can be applied to people who use a computer to commit them as well as to those who commit them without the use of a computer or network (Parker 1998, p. 114).

In other cases, the crime is unique and came into existence with the advent of the network. Hacking into computer systems is an example; while it might be linked to breaking and entering a home or business building, the elements that comprise unauthorized computer access and physical breaking and entering are different.

Most US states have laws pertaining to computer crime. These statutes are generally enforced by state and local police and might contain their own definitions of terms. The Texas Penal Code's Computer Crime section, defines Breach of Computer Security as "A person commits an offence if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner".

California Penal Code, on the other hand, defines a list of eight acts that constitute computer crime, including: altering, damaging, deleting, or otherwise using computer data to execute a scheme to defraud; deceiving, extorting, or wrongfully controlling or obtaining money, property, or data using computer services without permission; disrupting computer services; assisting another in unlawfully accessing a computer; or introducing contaminates into a system or network. Thus, the definition of cybercrime under state law differs, depending on the state. Perhaps we should look to international organizations to provide a standard definition of cybercrime.

At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined as:

(a) in a narrow sense: any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.
(b) in a border sense: any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or disturbing information by means of a computer system or network.

These definitions, although not completely definitive, do give us a good starting point on what we mean by *cybercrime*. Cybercrime, according to these definitions, involves computers and networks. In cybercrime, the "cyber" component usually refers to perpetrating qualitatively new offences enabled by information technology or integrating cyberspace into more traditional activities. Having defined the concept of cybercrime, it becomes necessary to compare it with traditional crime.

This involves examination of its characteristics, what makes it vulnerable to being manipulated, and the reports that have been conducted on its incidence and the damage it inflicts.

1.1.2 Contemporary Cybercrime

Cybercrime is one of the fastest growing areas of crime. More and more criminals are exploiting the speed, convenience and anonymity that modern technologies offer in order to commit a diverse range of criminal activities. In past, cybercrime has been committed by individuals or small groups of individuals. However, we are now seeing an emerging trend with traditional organized crime syndicates and criminally minded technology professionals working together and pooling their resources and expertise.

1.1.3 Terrestrial Crimes Versus Cybercrimes

The act of defining crime is often, but not always, a step toward controlling it. That is, the ostensible purpose of defining illegal behaviours as criminal is to make them liable to public prosecution and punishment (Crutchfield 2000, p. 7). Historically, "crime" was addressed at the local, community level of government (Hitchens 2003). Crime was small-scale, consisting of illegal acts committed by some persons that were directed against a victim. "Crimes", which were consistent across societies; fell into routinized, clearly-defined categories that reflected the basic categories of anti-social motivation, Crime was murder, robbery, and rape (Balckstone 1979).

Crime was also personal, if the victim and the offender did not know each other; they were likely to share community ties that put offences into a manageable, knowable context (Goodman and Brenner 2000, p. 151). This principle did not only facilitate the process of apprehending offenders—who stood a good chance of being identified by the victim or by reputation—but also gave citizens the illusion of security, the conceit that they could avoid being victimized if they avoided some activities or certain associations (Ibid). Law enforcement officers dealt with this type of crime because its parochial character meant investigations were limited in scope and because the incidence of crime stood in relatively modest proportion to the size of the local populace. Law enforcement's effectiveness in this regard contributed to a popular perception that social order was being maintained and that crime would not go unpunished (Ibid).

The development of ICTs in urbanization and in geographical mobility undermined this model to some extent, although it continued to function effectively for the most part. Legislators quickly adapted to the fact that ICTs could be used to commit fraud and to harass others. Because they modified their substantive criminal

law to encompass these activities, the old model still functions effectively for traditional real world crime.

Unlike traditional crime, however, cybercrime is a global crime. As a European Report explains:

> computer-related crimes are committed across cyberspace and don't stop at the conventional state-borders. They can be perpetrated from anywhere and against any computer user in the world.

In order to understand the sea of change ICTs introduce into criminal activity, it is important to consider a hypothetical: one can analogize a denial of service attack to using the telephone to shut down a supermarket business, by calling the business' telephone number repeatedly, persistently, without remorse, and thereby preventing any other callers from getting through to place their orders. On such a base, the vector of cyberspace lets someone carry out an attack such as this easily, and with very little risk of apprehension. It is so easy, in fact, that a 13 year-old hacker used a denial of service attack to shut down a computer company. Furthermore, in addition to the increased scale of criminal activity that cybercrime offers, it also has a tendency to evade traditional offence categories. While some of its categories consist of using ICTs to commit traditional crimes, it also manifests itself as new varieties of activity that cannot be prosecuted using traditional offence categories.

The dissemination of the "Love Bug" virus illustrates this. Virus experts quickly traced this virus to the Philippines. Using Information supplied by an internet service provider, agents from the Philippines' National Bureau of Investigation and from the FBI identified individuals suspected of creating and disseminating the "Love Bug". However, they ran into problems with their investigation: the Philippines had no cybercrime laws, so creating and disseminating a virus was not a crime. Law enforcement officers had no hard time convincing a magistrate to issue a warrant to search the suspects' apartment. Later on, moreover, the suspected author of the virus could not be prosecuted under the repertoire of offences defined by the Philippines criminal code.

Cybercrime's ability to morph into new and different forms of antisocial activity that evade the reach of existing penal law creates challenges for legislations around the world. Criminals have the ability of exploiting gaps in their own country's penal law in order to victimize their fellow citizens with impunity. Additionally, cybercriminals can exploit gaps in penal laws of other countries in order to victimize those nation's citizens, and others. As the "Love Bug" episode demonstrated, cybercrime is global crime.

1.1.4 Cybercrime and White Collar Crime

The definition of white collar crime has been an enduring topic of debate over the past century. Some are of the opinion that white collar crime is a "social rather than a legal concept, one invented not by lawyers but by social scientists". There is no

specific offence or group of offences that can be identified as white collar crime. As such, white collar crime is a concept similar to cybercrime in definitional difficulties (Smith et al. 2004, p. 10).

The traditional definition of white collar crime focused on crimes committed by persons of high status and social repute in the course of their occupation. Included in this definition were crimes committed by company officers, public servants, and professionals such as doctors and lawyers. The original emphasis was on economic crime, although over time, white collar crime has come to include any acts of occupational deviance involving a breach of the law or ethical principles. As such, it has been suggested that white collar crime now includes almost any form of illegality other than conventional street crimes (Ibid).

Technological developments over the past decade have created further complexities surrounding the types of persons able to commit white collar crime. The perpetration of an online fraud for example, might just as easily be a self-taught teenager using personal computer at home, as an educated professional in the workplace.

A simple categorisation distinguishes crimes committed by specified types of offenders from crimes perpetrated in specified ways. The essence of white collar crime, however, remains rooted in abuse of power and breach of trust, and usually involves the pursuit of financial gain as a motive (Ibid).

Clearly, not all white collar crimes involve the use of digital technologies, although in recent times the vast majority have done. Examples of those which do not include acts of violence committed in the workplace, such as the sexual assault of patients by doctors, and some environmental crimes, such as pollution (although even the later can be committed electronically).

The category of fraud or financial crimes of dishonesty intersects with white collar crime, economic crime, and cybercrime. Overlying these concepts are the categories of property crime and corporate crime. Property crime is sometimes used synonymously with economic crime, although trespass, for example, or acts of vandalism would not be economic, but nonetheless clearly property-related.

Problems also arise in relation to the types of property protected by criminal law. Notably, at least until recently, information has usually been regarded as being outside the scope of criminal prosecutions, dealt with instead by a range of intellectual property regimes such as copyright, patents, designs and protection of confidential information (Ibid).

1.2 The Scale of the Problem and Reasons for the Growth of Cybercrime

Knowing how much crime is committed might help us decide on how much to spend on security. Estimates by security experts of annual losses from computer crime range from $555 million to more than $13 billion (Parker 1998, p. 10), but

there are actually no valid statistics on the losses from this type of crime, because no one knows how many cases go unreported. Even when the victims of computer crimes are aware of the crimes, they are usually relocated to report their losses, especially if those losses can be easily hidden (UNESCO 2000). Victims can lose more from reporting crimes than they lose from the crimes themselves. Embarrassment, key staff diverted to prepare evidence and testify, legal fees, increased insurance premiums, and exposure of vulnerabilities and security failures can all result from reporting computer crime incidents (Parker 1998, p. 10).

As every aspect of commerce and communication has been changed by the Internet, crime has evolved to profit from the millions of potential victims connected to one global network. There are various reasons for the growth of cybercrime. First of all, the technology for cybercrime has become more easily accessible. Software tools can be purchased online that allow the user to locate open ports or overcome password protection. These tools allow a much wider range of people to become offenders, not just those with a special gift for computing. Cybercrime's place is growing due to the exponential connectivity, increased subject knowledge, cultural awareness, and programmable onboard electronics, which increase the number of potential targets. Compared to other crimes and offenses, it generally requires a smaller investment and can be carried out in various locations, without any geographical constraints, with no consideration to borders.

1.2.1 United States

The results of national surveys bear out the picture that cybercrime is consistently and dramatically on the increase. One of the famous cited national surveys for the United States is the "Computer Crime and Security Survey" conducted by the Computer Security Institute, with the participation of the San Francisco branch of the Federal Bureau of Investigation's Computer Intrusion Squad.

Key findings from the 2010/2011 CSI Computer Crime and Security Survey include:

- Almost half of the respondents had experienced a security incident, with 45.6 % of them reporting they had been subject of at least one targeted attack.
- Malware infection continues to be the most commonly experienced attack.
- Fewer financial frauds were reported than in previous years, with only 8.7 % saying they had seen this type of incident.
- Tools that improve visibility into networks, web applications, and endpoints were ranked among the highest on information security and information technology managers' 'wish lists', including better log management, security information and event management, security data visualization, and security dashboards.

The survey was conducted from July 2009 through June 2010 and respondents included US security practitioners from the private and public sectors. In 2010, IC3 received the second highest number of complaints since its inception, whilst also

reaching a major milestone this year when it received its two-millionth complaint. On average, IC3 receives and processes 25,000 complaints per month.

The most common victim complaints in 2010 were the non-delivery of payment/merchandise, scams impersonating the FBI and identity theft. Victims of these crimes reported losing hundreds of millions of dollars.

The 2010 Internet Crime Report demonstrates how pervasive online crime has become, affecting people in all demographic groups. The report provides specific details about various crimes, their victims and the perpetrators. It also shows how IC3 continually adapts its methods to meet the needs of the public and law enforcement.

1.2.2 United Kingdom

In the UK, the Office of Cyber Security and Information Assurance (OCSIA) works in partnership with Detica to look more closely at the cost of cybercrime and to gain a better appreciation of the costs to the UK economy of Intellectual Property (IP) theft and industrial espionage.

A study conducted considered three types of cybercrime that impact on individual citizens: identity theft; online scams and scareware.

The impact of identity theft was estimated in two ways, based on information published by CIFAS, in particular:

- The number of reported incidents was multiplied by the average cost of an incident and a further estimate made for the level of under-reporting;
- The number of UK citizens with internet access was multiplied by the probability that they became a victim of identity theft, modified by an estimate of the proportion of these crimes being conducted online (estimated at 25 %).

Both methods of calculation provided similar answers, with an average of £1.7 billion per annum. This compares well with the results of other studies by CIFAS, which also made an estimate of £1.7 billion per annum, and the IFSC, which reported a figure of £1.2 billion per annum.

Finally, the costs of scareware and fake anti-virus were calculated from information published by Symantec on the probability of such an attack and its average cost. The resulting figure of £30m was by far the lowest for any type of cybercrime, but it has been identified as an area of growth. The overall estimate for the economic cost of cybercrime to UK citizens is £3.1 billion per annum.

On a different note, the total estimate for industrial espionage is £7.6 billion. The results for different business sectors are shown below:

- aerospace and defence—£1.2 billion per annum—which is due to the large proportion of revenue that companies in this sector derive from large tendering competitions;
- financial services—£2.0 billion per annum—which is due to extremely high transaction volumes and recent share price fluctuations in this sector;

- mining—£1.6 billion per annum—which is due to both the increasing market value of raw minerals and the high level of mergers in this sector at present.

Although the existence of cybercrime in the UK economy appears endemic, efforts to tackle it seem to be more tactical than strategic. It is believed that the potential for reputational damage is inhibiting the reporting of cybercrime. The problem is compounded by the lack of a clear reporting mechanism and the perception that, even if crimes were reported, little can be done. Additional efforts by the Government and businesses to measure and improve their understanding of the level of cybercrime would allow responses to be targeted more effectively.

1.2.3 Middle East

In addition, many international sources are warning that the Middle East is becoming a major source of cybercrime; for example, Saudi Arabia is ranked as the leading country in the region as the target *and* source of malicious activities online; it is also the number one source of malicious attacks in the Gulf Cooperation Council (El–Guindy 2008, p. 17). Egypt is one of the *most phished* countries in the world with about 1,763 phishing incidents, followed closely by other countries in the region such as Saudi Arabia, the UAE and Qatar. It is not hard to see that cybercrimes are increasing in the region due to growth of user base with poor security awareness and the lack of regulations (Ibid). But even normal cybercrime, such as phishing, has its unique characteristics in Middle East. Due to religious motives and political issues in the region, hackers are successfully sending political or religious scams which urge users to open an email attachment, thereby infecting the computer with malware in order to attack Middle Eastern infrastructure targets such as e-commerce websites, banks, telecommunications and government services (Ibid).

Another important factor making the Middle East, and especially the GCC, a source and target of much cybercriminal activity is the growth of international banking and money laundering. The unique opportunities of a quickly developed financial infrastructure allowing anyone to transfer monetary funds to any country, anonymously and through tangled routes caught the attention of cybercriminals (Ibid). Electronic transfer is an efficient tool for concealing sources of money intakes and laundering illegally earned money. There are many well-known online money laundering cases involving victims in the Middle East who have been tricked in order to steal their identity or transfer money from their real accounts using phishing and scams. In one such example, the attacker might send a well-crafted link to users in the Middle East with an email conveying the message that there is a bulk sum of money someone wants to transfer to a UAE bank account. All too often users will reply to this scam, start to interact, and in the end become the victim.

Terrorist motivation plays a dramatic role in cybercrime in the Middle East as a communication tool and a weapon against an enemy (Ibid). Cyber terror is growing in the region due to religious, political and socio-economic issues, such as

unemployment. "Jihad Online" claims to use hacking as a technique to carry out jihad against their enemies. Cyber terrorists use their websites in many activities such as psychological warfare, propaganda, recruitment, fund raising, coordination of actions and data mining. One jihad website captures information about users who browse their websites (Ibid). Those who seem most interested in the group's cause or well-suited to carrying out its work are then contacted. Recruiters may also use more interactive internet technology such as online chat rooms and cybercafés, looking for receptive members of the public, particularly young people who have the religious motive that later can be converted to the terrorists' cause. IT professionals who can be influenced to help with the technology may also be sought. Electronic bulletin boards and forums are used as vehicles to reach out to potential recruits.

1.2.4 Asia/Pacific—Japan (APJ)

According to the Symantec Asia—Pacific Internet Security Threat Report, dated April 2010, the US is ranked first for overall malicious activity with 19 % of the total, while China ranked second worldwide, with 8 % (Symantec 2010, p. 3). In (Asia /Pacific—Japan) APJ, China ranked first for malicious activity in 2009, with 32 % of the regional total, down from 41 % in 2008. Due to population size, number of computer users, and high broadband penetration, the United States and China are always likely to rank highly. China has the most broadband subscribers in the world (significantly more than anywhere else in the APJ region) and malicious activity tends to increase in relation to growth in broadband infrastructure (Ibid).

The United States ranked first for originating attacks detected by APJ-based sensors in 2009, accounting for 26 % of all detected attacks, down from 28 % in 2008. Globally, the US also ranked first in 2009 for originating attacks against global targets in 2009, with 23 % of the worldwide total (Symantec 2010, p. 4), and again ranked first for web-based attacks globally in 2009, accounting for 34 % of the worldwide total. China ranked second globally in 2009, with 7 %, which is a decrease from 13 % in 2008. In the APJ region, although China ranked first for web-based attacks in 2009, its 37 % total for this reporting period is a significant decrease from 2008, when it accounted for 79 % of the total for the APJ region (Ibid).

In 2009, South Korea hosted the highest percentage of phishing URLs, with 43 % of the total. This is a substantial increase from 29 % in 2008, when South Korea ranked second behind China, which decreased to 12 % in 2009 from 35 % previously. Of the phishing URLs identified in South Korea in 2009, 91 % targeted the financial services sector (Symantec 2010, p. 5).

In 2009, 21 % of all spam detected worldwide originated in the APJ region. Within the region in 2009, India ranked first for originating spam, with 21 % of the regional total. In 2008, China ranked first, with 22 % of the regional total. Globally in 2009, India accounted for 4 % of spam detected, and ranked third (Ibid).

With regard to bot-infected computers, China ranked second, with 11 % of the worldwide total. In 2009 however, China ranked first for bot-infected computers in

the APJ region, accounting for 41 % of the total, which is a double-digit decrease from 58 % in 2008. The decrease in percentage in bot-infected computers in China is partly due to increases elsewhere in the APJ region, specifically in Taiwan and Japan, both of which significantly increased their percentages for bot-infected computers in the region in 2009.

Taiwan had the second highest percentage of bot-infected computers in the APJ region in 2009, with 28 % of the total. This is a significant increase from 2008, when 12 % of the region's bot-infected computers were in Taiwan. Globally in 2009, Taiwan accounted for 7 % of the worldwide total. Taipei, Taiwan was again the top city for bot-infected computers in APJ and worldwide in 2009, with 19 and 5 %, respectively. Taiwan has ranked second in this category in a number of reports (Symantec 2010, p. 10). The high bot activity in Taiwan may be due to the high broadband penetration there. Previously, the Symantec *Global Internet Security Threat Report* attributed this to the increasing levels of fiber-to-the-home/building (FTTH/B) deployment in Taiwan. As noted, malicious activity tends to grow with increased broadband capacity and FTTH/B connections currently provide the highest bandwidth capacities over traditional DSL or cable lines. Japan had the third-highest percentage of bot-infected computers in the APJ region in 2009, with 11 % of the total. This is an increase from 4 % in 2008, when Japan ranked fifth in the region. In 2009, Japan had 3 % of the global total for bot-infected computers, a high ranking that may be explained by its advanced internet infrastructure, as well as by the significant deployment of FTTH/B in the country (Ibid).

Worms were the most common type of malicious code observed in the APJ region in 2009, accounting for 5 % of the volume of the top 50 potential infections. This is an increase from 43 % in 2008, when worms ranked second to Trojans. It is also a higher percentage than the global total for worms of 43 % in 2009 (Symantec 2010, p. 11).

One of the primary contributors to this increase may be the rapid spread of the Downadup (a.k.a., Conficker) worm, which is designed with certain geolocation features that enable it to target specific regions, one of which is China. Eight of the top 10 malicious threats in the region in 2009 were worms, or had a worm component, up from seven in 2008. Moreoever, the volume of worm activity in the region increased by approximately 10 % in 2009. This increased worm activity also explains the degree of percentage decreases in the other threat types in the region in 2009 (Ibid). Most experts believe that common forms of computer related crime are significantly underreported because "victims may not realize that they have been victimized, may not realize that the conduct involved is a crime, or may decide not to complain for reasons of embarrassment or corporate credibility" (Ibid).

Other reasons for the under-reporting of cybercrime is mass victimization (caused by offences such as virus propagation), whereby: "the number of victims are simply too large to identify and count, and because such programs can continue creating new victims long after the offenders have been caught and punished". A final factor complicating the gathering and comparison of national crime statistics is that transnational computer related crimes are, by definition committed in, or have effects in, at least two states, hence risking multiple reporting or no reporting at all. Thus, much of the information we have on cybercrimes is the product of studies and

surveys addressed to individuals working in information security. On such a basis, the obvious problem arises that survey results include only the respondents of people who agreed to participate. Before basing critical decisions on survey information, it is important to find out what the response rate was; although there are no absolutes, in general we aim to trust survey results more when the response rate is high. Response rates for telephone surveys however, are often less than 10 %; while response rates for mail and e-mail surveys can be less than 1 %. It is not easy to make any case for random sampling under such circumstances, and all results from such low-response-rate surveys should be viewed as indicating the range of problems or experiences of the respondents rather than as indicators of population statistics.

1.3 Profiling Cybercriminals

People who intentionally abuse and misuse information cover a spectrum of criminals. Although it is impossible to characterize these criminals in a single profile, there are some interesting and useful criminal phenomena that we need to know in order to be effective in protecting information. Several of these characteristics differentiate cybercriminals from white-collar criminals.

1.3.1 Motives of the Cybercriminal

Although there is no way to describe a "typical" cybercriminal, Parker's interviews have revealed a number of common traits among these individuals (Parker 1998, p. 138). They are, for example, typically white-collar criminals who engage in fraudulent business practices associated with their otherwise legitimate occupations, e.g., a broker engaged in the sale of phony stocks. In psychological terms, they can be said to exhibit the differential association syndrome. They also frequently tend to anthropomorphize the computers that they attack, yet they assume that attacking a computer does no harm to people (Ibid). Many cybercriminals exhibit Robin Hood syndrome, rationalizing that they are taking from victims who—in their view—can afford it. This might also be viewed as attempting to achieve a commendable goal, at the expense of harming others.

1.3.2 How Cybercriminals Use the Network

Cybercriminals can use computers and networks as a tool for the crime, or incidentally to the crime itself. Many of the crimes committed by cybercriminals could be committed without using computers and networks. For example, terrorist threats could be made over the telephone or via postal mail; embezzlers could steal

company money out of the safe; con artists can come to the door and talk elderly individuals out of their savings in person (Shinder 2010, Online). Even those crimes that seem unique to the computer age usually have counterparts in the pre-internet era. Unauthorized access to a computer is technically different, but not so different in mindset, motives and intent from unauthorized access to a vehicle, home or business office (a.k.a. burglary). Defacing a company's web site is also in many ways very similar to painting graffiti on that company's front door (Ibid). Computer networks have done for criminals the same thing they've done for legitimate computers users: they've made the job easier and more convenient.

Some cybercriminals use the internet to find their victims. This includes scam artists, serial killers and everything in between. Police can often thwart these types of crimes and trap the criminals by setting up sting operations in which they masquerade as the type of victim that will appeal to the criminal. We tend to think of this in relation to crimes such as child pornography and pedophilia, but it's the same basic premise as setting up a honeypot on a network to attract the bad guys (Ibid).

In other cases, criminals use the networks for keeping records related to their crimes (such a drug dealer or prostitute's list of clients) or they use the technology to communicate with potential customers or their own colleagues in crime. Amazingly, a significant number of criminals use their own corporate laptops or email accounts to do this. This is a situation whereby IT professionals may stumble across evidence of a crime inadvertently—including crimes that are not, themselves, related to computers and networks (Ibid).

1.3.3 Types of Cyber Criminals

The cyber criminals consist of various groups and category. This division may be justified on the basis of the object that they have in their mind. The category of cyber criminals are shown below in Table 1.2.

Criminal profiling is the art and science of developing a description of a criminal's characteristics (physical, intellectual, and emotional) based on information collected at the scene of the crime. A criminal profile is a psychological assessment made before the fact—that is, without knowing the identity of the criminal. The profile consists of a set of defined characteristics that are likely to be shared by criminals who commit a particular type of crime. It can be used to narrow the field of suspects or evaluate the likelihood that a particular suspect committed the offence.

Though not quite that easy or certain in real life, criminal profiling is a valuable tool that can give investigations many clues about the person who commits a specific crime or series of crimes. Nonetheless, it's important to understand that a profile—even one constructed by the top profilers in the field—will provide only an idea of the general type of person who committed a crime; a profile will not point to a specific person as the suspect. Although good profiles can be amazingly accurate as to the offender's occupation, educational background, childhood experiences,

Table 1.2 Classification of cyber criminals

S. no	Category	Explanations
1	Children and adolescents between the age group of 6–18 years	The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other children in their group. Further, the reasons may be psychological even
2	Organised hackers	These kinds of hackers are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism etc.
3	Professional hackers/ crackers	Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further, they are even employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes
4	Discontented employees	This group include those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employee

material status, and even general physical appearance, there will always be many individuals who fit a given profile.

In *Scene of the Cybercrime* (Shinder 2002, p. 103), cybercriminals are classified into the following main categories.

1.3.3.1 Hackers, Crackers, and Network Attackers

The network is an important tool that makes white—collar criminals' and scam artists' jobs easier, but it is an absolutely essential tool for hackers. Unless a hacker has physical access to a computer with the Net, it would be impossible for him or her to commit a crime.

Hackers can commit several crimes, such as unauthorized access, theft of data or services, and destructive cybercrimes such as website defacement, release of viruses and DoS, and other attacks that bring down the server or network.

Hackers learn their "craft" in a number of ways: by trial and error, by studying network operating systems and protocols with an eye toward learning their vulnerabilities, and perhaps most significantly, from other hackers. There is an enormous underground network where those new to hacking can get information and learn from more experienced hackers.

There are numerous sites to meet hackers online, and many more that provide tools that can be used for hacking sites. Websites such as the Ethical Hacker

Network, Cult of the Dead Cow, Hacktivismo, Security Hacks, and Darknet provide information and software to discover vulnerabilities and access systems. Of course, almost any network security tool used for testing problems can be used for these purposes. In addition to this, there are newsgroups, mailing lists, online papers and videos that provide guidance and detailed information. Hacker conferences such as DEFCON and the Black Hat Briefings provide real world opportunities for hackers to meet. The hacker culture, furthermore, divides itself into two groups:

- *Black hats* break into systems illegally, for personal gain, notoriety, or other less–than—legitimate purposes.
- *White hats* write and test open source software, work for corporations to help them heighten their security, work for the government to help catch and prosecute black–hat hackers, and otherwise use their hacking skills for noble and legal purposes.

There are also hackers who refer to themselves as gray hats, operating somewhere between the two primary groups. Gray-hat hackers might break the law, but they consider themselves to have a noble purpose in doing so. For example, they might crack systems without authorization and then notify the system owners of the systems' fallibility as a public service, or find security holes in software and then publish them to force the software vendors to create patches or fixes for the problem.

Ethical hacking is a term used to describe hackers who use their skills to hack networks on behalf of the owners. Numerous courses train computer professionals in hacking systems, including the EC—Council's Certified Ethical Hacker (CEH) certification, courses, and even a Master's of Ethical Hacking and Countermeasures degree that is offered by the University of Abertay in Scotland.

If a hacker has the requisite skills, including the social skills necessary to function in the corporate world, ethical hacking can be a lucrative business. Consultants charge companies $10,000 or more to test their security by attempting to hack into their systems and providing recommendations on plugging the security holes that they find.

1.3.3.2 Criminals Who Use the Net Incidentally to the Crime

Some criminals use the network in relation to their crimes, but the Net itself is not an actual tool of the crimes. That is, the network is not used to commit the criminal activity, although it can be used to prepare for or keep records of the criminal activity. Examples of this type of criminality include:

- Criminals who use the Net to find victims
- Criminals who use computers or networks for recordkeeping
- Criminals who use email or chat services to correspond with accomplices.

Even in cases in which the network is not a tool of the crime, it can still provide evidence of criminal intent and clues that help investigators track down the criminals. We discuss each situation in the following paragraphs:

In the first category, criminals go on to use the internet to actually commit the crime, for example, sending electronic chain letters, emailing fictitious notices purporting to be from the victim's ISPs that request their credit card information, or directing victims to a website that tries to sell them products under false pretenses. In these cases, the internet is a tool of the crime, but the initial act of searching out potential victims is not, by itself, criminal. Thus, a pedophile or rapist or other criminals who use the Net to find victims but then commit the criminal activity in the real world are using the internet incidentally to the crime. However, the internet can also be used to step up a sting operation that will turn the tables and lure the criminal into revealing his or her identity to law enforcement.

The second category includes people who engage in non-computer-related criminal activity such as drug dealing, illegal gambling, or other illicit businesses, who use computers to keep financial records, customer lists, and other information related to the criminal activity, whilst simultaneously utilizing the internet to transfer those files to an off-site location where they will be safer from law enforcement.

Transferring business records to a friend's computer or an internet data storage service is not against the law, so internet use is incidental to this criminal activity, even though the files in question might be important evidence of the crime itself.

The last category includes criminals who work in groups—terrorist groups, theft rings, black hat hackers—often use emails and chats in the same way that legitimate users do: to correspond with people they work with. The correspondence itself is not a crime; it is the illegal activity being planned or discussed that is criminal. However, the correspondence can be used not only to show the criminal's intent and help track the offender down, but also, in some cases, to prove the existence of a criminal conspiracy. This is important because if the elements of conspiracy exist, charges can be brought against all members of the conspiracy, not just the person(s) who physically committed the crime.

1.3.3.3 Real-life Noncriminals Who Commit Crimes Online

In some situations, people who are not criminals in real life engage in criminal conduct online. These include accidental cybercriminals and situational cybercriminals. *Accidental cybercriminals* have no criminal intent. They commit illegal acts online because of ignorance of the law or lack of familiarity with the technology. An example is someone who has a cable modem connection or is using the broadband internet access available in some hotels and opens the Network Neighbourhood folder on his computer and sees other computers listed there. Curious, he might click on the icons just to see what happens. If he has stumbled upon a computer on the network that is running a low-security operating system or doesn't require a username and password to log on, and it has network file sharing enabled, he might be able to access the shared files on that computer.

If our hypothetical user is not very technically or legally savvy, he might not even realize that those files are on someone else's private computer. Or he might think that because they're accessible, it is legal to look at them. However, depending on how

the state's or country's unauthorized access statutes are written, it might be a crime to access any other computer across a network without permission, even if that computer's users have, perhaps unwittingly, made it technologically easy to do so.

1.4 Challenges for Criminal Justice and Law Enforcement

The internet facilitates the ability of offenders to communicate directly with other likeminded persons as well as future victims through chat rooms, newsgroups, internet relay channels, websites and emails (Fantino 2009, Online). The high volume of offences on the internet and the lack of international boundaries require the cooperation and sharing of information between and among national and international police departments, government legislators, and the public and private sectors (Ibid). This powerful medium is proving to be one of the greatest challenges law enforcement has ever had to deal with. In the following section we shall provide a brief overview of the major challenges in fight against cybercrime.

1.4.1 Transnational Legal Jurisdictions

Domestic legislation is clearly necessary to target cybercrime offenders; however, various problems with the way that cybercrime is now committed make the use of domestic regulation by itself unworkable (Smyth 2007, p. 59). Acts on the internet that are legal in the country where they are initiated, may be illegal in other countries, even though the act is not particularly targeted at that single country (Ibid). Jurisdiction conflicts abound, both negative (no country claims jurisdiction) and positive (several countries claim jurisdiction at the same time). Above all, it is unclear just what constitutes jurisdiction: is it the place of the act, the country of residence of the perpetrator, the location of the effect, or the nationality of the owner of the computer that is under attack? Or, all of these at once? (Ibid).

1.4.2 Evidence Identification and Tracking

The dynamic and distributed nature of cyberspace makes it difficult to find and collect all relevant digital evidence of cybercrimes. Data can be spread over cities, states or even countries. When dealing with the smallest networks, it is feasible to take a snapshot of an entire network at a given instant (Casey 2004). Furthermore, network traffic is transient and must be captured while it is in transit. Once it is captured, only copies remain and the original data are not available for comparison (Ibid). Although the amount of data lost during the collection process can still be documented, the lost evidence cannot be retrieved. Once it is captured, only copies remain and the original

data are not available for comparison. Furthermore, open networks contain large amounts of data and sifting through them for useful information can be like looking for a needle in a haystack and can stymie an investigation (Ibid).

1.4.3 Tactics for Evasion

A further set of problems arise where an offender is using encryption. There are several means by which this might take place. In the most common, parts of the suspect's stored data are encrypted—most of the PC is "open" but there are directories, sections, files, or "containers" which hold files, which are encrypted (Sommer 2002). This approach is popular because it is easy to implement and there are relatively large numbers of robust software products available; the computer can be used normally and then specific actions are needed to decrypt the "secret" items (Ibid). Furthermore, some IRC clients support encryption, making it more difficult for investigators to monitor communications and recover digital evidence (Ibid).

Offenders can make it more difficult to locate them on IRC by using the invisibility feature (Casey 2004). This feature does not conceal the offender from other internet users in the same channel, however, so offers only limited protection. One advanced aspect of IRC that some criminals use to conceal their IP address are "bots" (Casey 2004). These programs can work like proxies and are used to perform various tasks from administering a channel to launching denial of service attacks. "Eggdrop" is one of the more commonly used IRC bots and can be configured to use strong encryption that conceals the contents of its logs and configuration files making it necessary to examine network traffic to observe nicknames and passwords (Casey 2004). Finally, cyber offenders who are more technically savvy and are especially interested in concealing their identity, send messages through anonymous or pseudonymous services. When an email is sent through an anonymous remailer, identifying information is removed from the email header before sending the message to its destination (Ibid). The most effective anonymous remailers are quite sophisticated and make it very difficult to determine who sent a particular message. Some remailers keep logs of the actual email addresses of individuals, but many of them will perish than make such concessions, even when illegal activity is involved. There is a possibility that investigators can compel a pseudonymous remailer to disclose the identity of the sender but it requires significant effort since their business is to protect the identity of their users (Ibid).

1.5 The Future of Cybercrime

In the growing world of the internet, both in personal and internet businesses, cybercrime is an ever increasing problem. Punishment for these crimes has become a new field in crime investigation and law enforcement. Cybercrime has taken

criminals across borders and limitations that nothing else has been able to, until the advent of the internet. Where a door is left open, the criminal element will find their way in. In this case, the door for crime is the internet.

Cybercrime is vast in scope. It ranges from the individual criminal, to an increasing presence of International Organized Cyber Crime. Scams run rampant across the internet. They fill email boxes and websites, trying to lure unsuspecting victims into their webs of deception. Spy bots and Trojan programs attempt to infiltrate sensitive personal and business information, to gather what they can find, to be used with criminal intent.

Crimes of a more personal nature also abound across the internet. Dating and chat sites are rife with scammers or people playing dangerous games with individual human victims. This social interaction becomes a crime when the person is victimized by cyber stalkers, or people who use the internet to bolster their insecurities, at the expense of acting like a real human being. Regrettably, children are often the victims of such crimes. News headlines, moreover, often include stories of victims to these internet or cybercrimes. Some victims have reacted in personal desperation to violations perpetrated by the online stalkers and game players.

Maintaining security and safety on the internet has become increasingly more complex. Whole companies and businesses exist to deal with the problems.

What's in the future for internet crime and punishment? With every new avenue opening up on the internet comes more possibilities for criminal intent. The difference now, and the future, is that technology and human services are either in place or coming into place, to make these individuals and organizations accountable for their actions. Laws and punishments for even the smallest internet crimes are now on the books, or in the process of being created. Make no mistake, once something is on the internet, it is fact. It is traceable and punishable. No matter how hard someone tries to cover it up, erase it or disassociate from their actions, once the footprint is made, it can't be unmade. Somewhere there is a way to track that footprint. Law enforcement across the globe will enforce it.

The internet has not only drawn people together, it has drawn international crime fighting agencies together in a common purpose. The internet is not a free playground anymore. It is a global arena.

1.6 Summary

It is clear that cybercrime is a growth industry internationally. Precisely because of its international nature, such crimes create many political and jurisdictional problems and problems arising from the incompatibility of criminal and criminal-procedure codes.

Therefore, it is of the greatest importance that Arab countries ratify international documents such as the Convention on Cybercrime. Failing to do this will create "crime shelters" similar to "tax shelters" created by the legislation in certain states.

Furthermore, without the necessary political will and corresponding funding for the required administrative structures, many countries will quickly become an easy target for international cybercrimes.

References

W. Blackstone, *Commentaries on the Laws of England* (University of Chicago Press, Chicago, 1979)
E. Casey, *Digital Evidence and Computer Crime* (Elsevier Academic Press, California, 2004)
R. Crutchfield, *Crime: Readings* (Pine Forge Press, California, 2000)
M. El–Guindy, Cybercrime in the Middle East. ISSA J. 17 (June, 2008)
J. Fantino, Child pornography on the internet: new challenges require new ideas. Police Chief Mag. (2009), http://policechiefmagazine.org. Accessed 23 July 2011
D. Goodman, S. Brenner, The emerging consensus on criminal conduct in cyberspace. Int. J. Law Inf. Technol. **10**(2), 3 (2002)
P. Hitchens, *A Brief History of Crime* (Atlantic Publishing, London, 2003)
D. Parker, *Fighting Computer Crime: For Protecting Information* (Wiley, New York, 1998)
D. Shinder, *Scene of the Cybercrime* (Walthman, Syngress, New York, 2002)
D. Shinder, Profiling & categorizing cybercriminals (2010), http://www.techrepublic.com. Accessed 10 July 2011
R. Smith, P. Grabosky, G. Urbas, *Cyber Criminals on Trial* (Cambridge University Press, Cambridge, 2004)
S. Smyth, Mind the gap: a new model for internet child pornography regulation in Canada (2007), http://www.sfu.ca. Accessed 11 July 2011
P. Sommer, in *Evidence in internet pedophilia cases*. NCS/ACPO Conference, July 2002, Bournemouth, http://www.pmsommer.com. Accessed 01 July 2011
Symantec, Symantec internet security threat report (2010), http://www.symantec.com. Accessed 8 July 2011
UNESCO, *Les Dimensions Internationales du Droit du Cyberespace* (Economica, Paris, 2000)