Dealing with the Problem of Cybercrime

Ali Alkaabi, George Mohay, Adrian McCullagh, and Nicholas Chantler

Information Security Institute, Queensland University of Technology, GPO Box 2434, 126 Margaret Street, Brisbane, QLD 4001, Australia
a.alkaabi@isi.qut.edu.au,
{g.mohay,a.mccullagh,a.chantler}@qut.edu.au

Abstract. Lack of a universally accepted and comprehensive taxonomy of cybercrime seriously impedes international efforts to accurately identify, report and monitor cybercrime trends. There is, not surprisingly, a corresponding disconnect internationally on the cybercrime legislation front, a much more serious problem and one which the International Telecommunication Union (ITU) says requires 'the urgent attention of all nations'. Yet, and despite the existence of the Council of Europe Convention on Cybercrime, a proposal for a global cybercrime treaty was rejected by the United Nations (UN) as recently as April 2010. This paper presents a refined and comprehensive taxonomy of cybercrime and demonstrates its utility for widespread use. It analyses how the USA, the UK, Australia and the UAE align with the CoE Convention and finds that more needs to be done to achieve conformance. We conclude with an analysis of the approaches used in Australia, in Queensland, and in the UAE, in Abu Dhabi, to fight cybercrime and identify a number of shared problems.

Keywords: Cybercrime, Computer Crime, CoE Convention on Cybercrime.

1 Introduction

Grabosky, Smith and Dempsey [1] note that the "fundamental principle of criminology is that crime follows opportunity, and opportunities for theft abound in the Digital Age". Grabosky [2] indicates that the growth of computer technology and the Internet have increased the opportunities for criminals to commit cybercrime. While the general problem posed by cybercrime has been known and identified for sometime now, there are markedly different interpretations of the nature of cybercrime [3]. Cybercrime has historically referred to crimes happening specifically over networks, especially the Internet, but that term has gradually become a general synonym for computer crime, and we use these two terms as synonyms except where we make explicit otherwise. Another synonym still, one that is increasingly being used, is the term 'hi-tech crime' which makes explicit that such crimes include crimes involving any device incorporating an embedded digital device. Unfortunately, in developing more detailed and precise definitions and taxonomies, different countries and national and international organizations have given rise to diverse and often inconsistent definitions and taxonomies. In fact, the United Nations (UN) [4] noted that the problems surrounding international cooperation in the area of computer crime include the lack of global agreement on what types of conduct should be designated as computer crime and the lack of

I. Baggili (Ed.): ICDF2C 2010, LNICST 53, pp. 1–18, 2011.

global agreement on the legal definition of criminal conduct. Without common agreement or understanding on cybercrime definitions and taxonomy, it is difficult to report on its nature and extent consistently from one country to another, and to monitor trends in an informed manner. Furnell (2001) [3] notes that having a consistent classification of cybercrime would be beneficial to individuals and organizations concerned with countering the problems of cybercrime, and to those concerned with reporting these kinds of offences. The G8 [5] has recommended each country to map its high-tech crime taxonomy to "make it addressable with other countries".

Section 2 of the paper discusses the variety of terms, definitions and taxonomies used to describe cybercrime, including ones used by international organizations such as the UN and Council of Europe (CoE). Section 3 presents our refined and extended cybercrime taxonomy and demonstrates its utility and broad applicability. Section 4 explores the influence of the CoE Convention on Cybercrime (CoE Convention) internationally by analysing how the USA, the UK, Australia and the UAE[1] conform to the CoE Convention. These four countries represent a spectrum of development and culture and have been chosen partly for those reasons. Our results show not surprisingly that more needs to be done in order to address harmonization of cybercrime legislation amongst these four countries and, by extension, globally. As part of our analysis of how the fight against cybercrime is proceeding globally, Section 5 concludes the paper with a comparison of the approaches used by the Queensland Police Service in Australia and by the Abu Dhabi Police service in the UAE to fight cybercrime. The analysis shows that resourcing is a problem, and so too is reporting of cybercrime.

2 Terminology and Taxonomies

There are, at present, a large number of terms, definitions and taxonomies proposed or used to describe crime involving computers. The terms include *computer related crime*, *computer crime*, *Internet crime*, *e-crime*, *digital crime*, *technology crime, high-tech crime*, *online crime*, *electronic crime*, *computer misuse*, and *cybercrime*. The latter has been widely used recently [3, 6-13].

Symantec Corporation [14] defines cybercrime broadly as "any crime that is committed using a computer or network, or hardware device". This is a very broad definition that not only includes crimes that use or target computer systems and networks, but it also includes crimes that happen within a standalone hardware device or computer. Kshetri [15] analyses cybercrime and its motivation in terms of cost-benefit to the cyber-criminal and defines cybercrime as a crime that utilizes a computer network during the committing of crimes such as online fraud, online money laundering, identity theft, and criminal uses of Internet communication. Wall [16] describes cyberspace and the new types of crime as "new wine, no bottles", however, in contrast, Grabosky [17] suggests that it is a matter of "old wine in new bottles", since the cybercrime is "basically the same as the terrestrial crime with which we are familiar". However, generally and as indicated previously, the term 'cybercrime' involves not only new crimes against computer data and systems, but it also involves traditional crimes such as fraud.

[1] This research is funded by the Abu Dhabi Police, UAE.

The CoE Convention classifies cybercrime into four main categories [18]: offences against confidentiality, integrity and availability of computer systems and data; computer related offences (forgery, fraud); content related offences; and offences related to infringements of copyright and related rights. We note that the CoE cybercrime categorization does not include some types of crimes that have been committed or facilitated using the computer such as money laundering, identity theft and storing illegal content.

The UN manual on the prevention and control of computer-related crime [4], published in 1999, lists five common types of computer crime: fraud by computer manipulation; computer forgery; damage to or modification of computer data or programs; unauthorised access to computer systems and services; and unauthorised reproduction of legally protected computer programs. Though the UN manual includes crimes against computer data and systems, it also covers some crimes that utilize computer systems such as fraud and forgery. However, the manual does not refer to other types of offences that are committed or facilitated by a computer or computer system such as identity theft, money laundering and storing illegal content.

The U.S. Department of Justice defines [19] *computer crimes* as "crimes that use or target computer networks, which we interchangeably refer to as 'computer crime,' 'cybercrime,' and 'network crime'", and refers to viruses, worms and Denial of Service attacks. The UK Association of Chief Police Officers (ACPO) [20] has defined e-crime as the "use of networked computers, telephony or Internet technology to commit or facilitate the commission of crime", which is consistent with the original, network-specific, origins of the term cybercrime.

The above terms and others are often used interchangeably to describe the same crimes [6, 21], nonetheless there is an ongoing debate on the specific kinds of crime encompassed by cybercrime. Brenner [22] classifies cybercrime into three categories: the use of a computer as a target of criminal activity (e.g., hacking, dissemination of viruses and worms), the use of a computer as a tool or instrument used to commit a criminal activity (e.g., online fraud, harassment), and the use of a computer as incidental to the crime (e.g., data storage for a drug dealer to monitor sales and profits). Some others concur with this view (Symantec Corporation [14], Gordon and Ford [8], Sukhai [23], Kelly [7], and the Australian Centre for Police Research [21]). Still others however classify cybercrime into only two categories (see Koenig [24], Furnell [3], Wilson [25], Lewis [26], and the Australian High Tech Crime Centre [27]). Similarly, the Foreign Affairs and International Trade of Canada [12] classifies cybercrime into two categories: crime that is committed using computers and networks (e.g., hacking and computer viruses) and traditional crime that is facilitated through the use of computers (e.g., child pornography and online fraud). The crimes which cover the indirect use of computers by criminals (e.g., communication, document and data storage) are termed computer-supported crime and not cybercrime [12]. Likewise, the categorization by Urbas and Choo [28] identifies two main types of cybercrime: crimes where the computer is a target of an offence (e.g., hacking, terrorism) and crimes where the computer is a tool in the commission of the offence (e.g., online fraud, identity theft). Urbas and Choo elaborate the second type, the computer as a tool, based upon the level of reliance on technology: computer-enabled crimes, and computer-enhanced and computer-supported crimes.

Other classifications still have included consideration of factors other than the role a computer system plays in the committing of computer-related crimes. These factors include: threats (Thomas [29]), attackers (Kanellis et al [30]), attacks (Kanellis et al [30], Chakrabarti and Manimaran [31]), motives (Kanellis et al [30], Thomas [29] and Krone [32]), and victims (Sukhai [23]).

In summary, the overridingly predominant view is clearly that for a crime to be considered as cybercrime, the computer or network or digital device must have a central role in the crime i.e., as target or tool. This precludes crimes in which the computer has only an *incidental* role such as being the repository of either direct or circumstantial evidence of the crime and Section 3 of this paper is therefore based upon the premise that cybercrimes involve a computer system or network or digital device in one or both of the following two roles:

- *Role I*: the computer is a target of a criminal activity
- *Role II*: the computer is a tool to commit a criminal activity.

3 A New Model for Classifying Cybercrime

This Section presents the development of a more comprehensive model to characterize cybercrime based not only upon the role of the computer, but also on the detailed nature of the crime, and contextual information surrounding the crime. Sub-section 3.1 refines the Role I/II classification of cybercrime, which we will henceforth refer to as the Type I/II classification, into a number of sub-classes and uses that refined classification scheme to categorize a comprehensive list of common cybercrimes. Sub-section 3.1 also discusses how cyber-terrorism offences fit that refined classification. Sub-section 3.2 presents the case for an extended model which also incorporates contextual information such as main motive/offender role, the offender relationship, and scope of impact, as well as the role of the computer and presents a detailed analysis of a number of significant cybercrime case studies using that model to illustrate its expressiveness.

3.1 Refining the Type I/II Classification of Cybercrime

The purpose of reviewing and investigating different definitions and classifications of computer crime is to determine a consistent and comprehensive taxonomy that will benefit the organizations that deal with combating such crimes. Some of the benefits include: sharing of information, accurate reporting of cybercrime cases, cooperation on actual cases, cooperation on combating cybercrime, and harmonization of cybercrime regulation and legislation. The UN classification of computer crime addresses some main categories of crimes involving computers without considering other types of offences such as copyright and harassment. The CoE computer crime taxonomy is a broader classification. However, the CoE cybercrime classification too does not include a number of other types of crimes that are supported or facilitated using computers such as money laundering and identity theft.

We have further below consolidated a comprehensive list of crimes which are generally regarded as cybercrime and classified them according to the Type I and Type II

classification. In doing so we have identified different sub-classes for both Type I and Type II offences. These sub-classes appear to us to be intuitive and enable us to arrive at a natural classification of that list of cybercrimes. Some of the previous work on classifying cybercrime reviewed in Section 2 has likewise extended to sub-classes but that work has either by-passed the major Type I/II classification (e.g., CoE [26]), focused solely on computer attacks *per se* (e.g., Kanellis et al [20]), or has merged crimes where the role of the computer is merely incidental to the crime into Type II (e.g., Urbas and Choo [36]). Our sub-classes build on and consolidate some of that previous work to provide a more comprehensive and expressive model. We now describe our refined taxonomy:

Type I crimes include crimes where the computer, computer network, or electronic device is the ***target*** of the criminal activity. We divide this into four sub-categories:

- Unauthorized access offences [4] such as hacking
- Malicious codes offences [5] such as dissemination of viruses and worms [22]
- Interruption of services offences [24] such as disrupting or denying computer services and applications such as denial of service attacks and Botnets
- Theft or misuse of services [28, 33] such as theft or misuse of someone's Internet account or domain name [24].

Type II crimes include crimes where the computer, computer network, or electronic device is the ***tool*** used to commit or facilitate the crime. We divide this category into three sub-classes:

- *Content violation offences* [33] such as possession of child pornography, unauthorized possession of military secrets, IP offences
- Unauthorised alteration of data, or software for personal or organisational gain [34] such as online fraud
- Improper use of telecommunications [22] such as cyber stalking, spamming, and the use of carriage service with the intention or conspiracy to commit harmful or criminal activity.

We present this refined taxonomy and a list of common examples of cybercrime classified according to the refined taxonomy in Fig. 1. It is clear that in some of these crimes, the computer plays multiple roles and hence that one crime can be classified under multiple types, however there will typically be one primary role, and hence one primary cybercrime type classification by which to classify the crime. As a result, the categories of Fig. 1 are not necessarily exclusive. This corresponds naturally to the reality that there may actually be several separate offences involved in the one case.

Cyber-terrorism and critical infrastructure attacks pose some interesting issues worthy of further consideration. According to Wilson [25], the U.S. Federal Emergency Management Agency (FEMA) defines 'cyberterrorism' as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives". Coleman [35] defines 'cyberterrorism' as "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives".

According to the UK Parliamentary Office of Science and Technology [36], cybercriminals may use computers to "damage the functioning of the Critical National Infrastructure (CNI) which includes emergency services, telecommunications, energy distribution and finance, all of which rely on IT". The Australian High Tech Crime Centre [27] categorized cyberterrorism under Type II along with fraud, money laundering and other traditional crimes. Others [25] have considered physical attacks (not using a computer) against critical infrastructure such as Internet, telecommunications, and electric power grid as cyberterrorism.

It seems evident that any attack against a computer and computer network intended for political purposes is a cybercrime and can be labeled as cyberterrorism and Urbas and Choo [28] have indeed categorized cyberterrorism-related offences under Cybercrime Type I. In fact, any offence that comes under Cybercrime Type I could be considered cyberterrorism if the intent of the attacker is to commit a terrorism act. The FEMA and Coleman definitions of cyberterrorism indicate that some Cybercrime Type II offences can be considered cyberterrorism, depending upon the intent of the attacker (e.g., theft of military secrets). We note therefore that cyber-terrorism may involve offences of both Type I and Type II, for instance, a cyberterrorist needs first to attack a computer or a computer network and misuse computer services in order to get at the power grid. As a result, there are two types of cybercrime in this terrorist act: Type I and Type II.

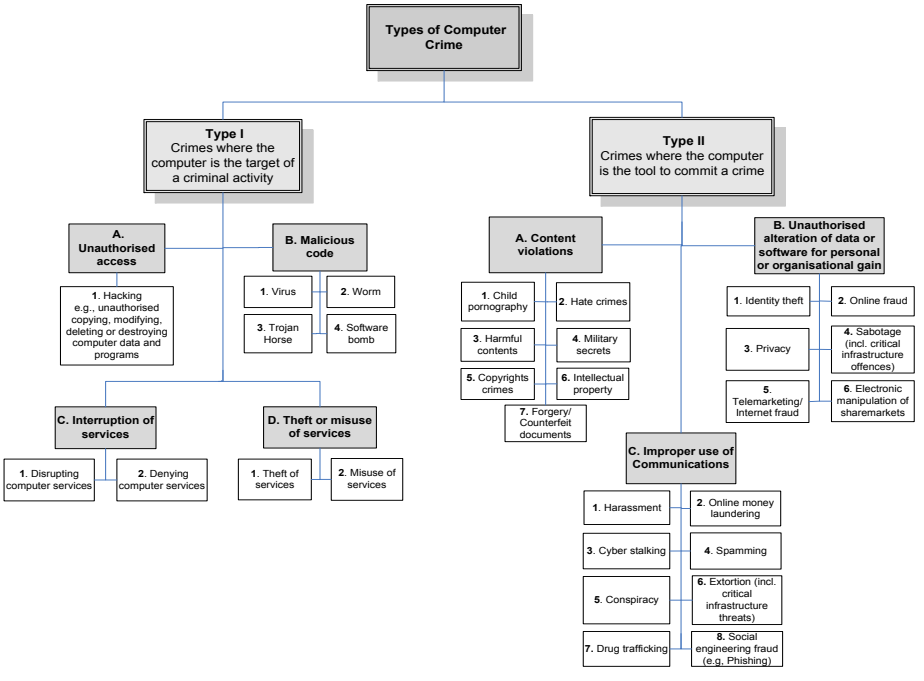

Fig. 1. Refined cybercrime classification

3.2 Extending and Applying the Refined Taxonomy

The question to be asked at this point is how accurately and completely does the above refined classification, illustrated in Fig. 1, depict actual cases of cybercrime? This classification based on identifying the type of the cybercrime and the role/s of the computer in the crime omits to consider some important contextual information such as main motive/offender role, and the offender relationship and scope of impact. Identifying such additional markers promises to be important for government and international bodies who work in the area of crime trends and analysis, and who set strategies to counter and prevent such crimes. We therefore focus in this Sub-section on analysing and investigating some cybercrime cases in more detail, including not just the type of cybercrime in terms of (the refined) Cybercrime Types I and II , but also contextual information regarding main motive/offender role, the offender relationship, and scope of impact. In analysing these cases, we assessed the following characteristics of each offence:

- *The type of cybercrime*: which type or types of cybercrime have been committed (Cybercrime Type I/II)
- *Refined classification*: where does each offence appear in the detailed classification represented in Fig. 1
- *Main motive/offender role*: what are the motives of the offence; is it an individual's motivation, or is it a politically related crime such as information warfare, or terrorism activity, or that of an organized crime group
- *The offender relationship*: how can we classify the offender's relationship to the victim, are they from inside, or outside
- *The scope of impact*: what is the scope of impact of the offence, is the victim or target an individual, business, government agency or global infrastructure such as the Internet.

We have analyzed the following well-known cybercrime case studies according to the refined Type I/II classification scheme and contextual markers identified above:

- Morris worm [37]
- Maroochydore public waterways sewage [38]
- Harassment letter send by email
- U.S. v. Gorshkov & U.S. v. Ivanov [39, 40]
- Fungible credentials [41]
- International Interpol-led investigation on child pornography [42]
- ShadowCrew [43]
- Holiday prize scam [44]
- Fraud and money laundering scheme [45].

Identifying not only the specific nature but also the contextual information of cybercrime in this way is useful to organizations setting strategies and plans to counter cybercrime. We have summarised the results of our analysis in Table 1. Table 1 captures the essential features of the crimes analysed and provides a concise but sufficient description of each crime so as to enable informed reporting and accurate statistical analysis of the nature of the cybercrimes involved. We believe this demonstrates the applicability and utility of the extended refined taxonomy.

4 International Cybercrime Legislation and Compliance with CoE Convention

We focus on the criminal law provisions of the CoE Convention, Articles 2 to 11:

- Articles 2 to 6 in relation to the offences against the confidentiality, integrity and availability of computer data and systems
- Articles 7 and 8 regarding computer related fraud and forgery
- Article 9 concerning content related offences
- Article 10 concerning offences related to infringements of copyright, and
- Article 11 regarding the auxiliary liability and sanctions.

Table 1. Characteristics of some cybercrime case studies

Case #	Case name/detail	Type of computer crime	Refined classification (Fig. 1)	Main motive/offender role	Offender relationship	Scope of Impact
1	Morris worm	Type I	I.B2, I.C1	individual	outsider	Business, government and the Internet
2	Maroochydore public waterways sewage	Type I	I.A1	individual	outsider	Business and government
3	Harassment letter send by email	Type II	II.C1	individual	outsider	individual
4	U.S. v. Gorshkov U.S. v. Ivanov	Type I and Type II	I.A1, II.B2, II.C5, II.C6,	Individuals and organised crime	outsider	business
5	Fungible credentials	Type II	II.A7	Individuals and organised crime	outsider	individuals
6	International Interpol-led investigation on child pornography	Type II	II.A1	Individuals and organised crime	outsider	individuals
7	Shadowcrew	Type I and Type II	I.A1, I.D1, II.B1, II.B2, II.C8	Organised crime	outsider	Individuals and business
8	Holiday prize scam	Type II	II.B2, II.C8	Organised crime	outsider	Individuals
9	Fraud and money laundering scheme	Type II	II.B2, II.C2, II.C5	Organised crime	outsider	Individuals

Source: Markoff [37], Wyld [38], CIO Asia [39], Attfield [40], Berghel [41], Ninemsn [42], Grow & Bush [43], SCAMwatch [44] and the U.S. Department of Justice [45].

In this section we provide a comparative review of the computer crime and cybercrime legislation used in Australia, the UAE, the UK and the USA in the context of the CoE Convention. It compares the federal computer crime and cybercrime legislation of Australia, the UAE, the UK and the USA, and in particular determines whether and to what extent each of these jurisdictions corresponds to the criminal provisions provided by the CoE Convention, Articles 2 to 11. This section aims to identify the existence of legislation in these four countries that corresponds to the CoE Convention. It also comprises a comparative review of cybercrime legislation enacted in Australia, the UAE, the UK and the USA that aligns with the criminal provisions provided by the CoE Convention.

The findings show that Australia, the UAE, the UK and the USA have federal legislation that covers all the CoE Convention Articles 2 to 11, and the UAE covers all but one – Article 6. We observe also:

- While these four countries have provisions on criminalising offences identified under Articles 2 to11, not all of these offences are criminalised under the one legislation, but rather under different legislations
- With regard to criminal sanctions, all of the four countries provide provisions for the punishment of committing the CoE Convention related offences but that there are some variations in the penalties for committing computer-related offences in these four countries. The USA legislation has provision for longer and tougher penalties. In contrast to the UAE, the UK and the USA, committing one of the computer offences in Australia is more likely to be punished with only an imprisonment term. Also, the UAE criminal sanctions system has smaller and lighter punishments compared to the other countries.

Table 2 lists the cybercrime provisions in Australia, the UAE, the UK and the USA corresponding to the CoE Articles. Additionally, Table 3 illustrates the penalties for committing these offences in Australia, the UAE, the UK and the USA.

In a further step, we investigated the degree of alignment of the legislation with the Articles as presented in Table 4. This is a preliminary evaluation only, a detailed and comprehensive evaluation is outside of the scope of this work and a subject for further work. Each Article 2 to 11 of the CoE Convention has essential criteria such as that the crime must be committed 'intentionally' and 'without right'. In reviewing the legislation we assessed it against these essential criteria. Table 4 shows the results of the preliminary analysis. It is apparently the case that the degree of alignment with Articles 2 to 11 of the CoE Convention as represented in Table 4 is low in Australia and the UK and very low in the UAE.

The USA alignment truly reflects its involvement from the beginning in the development of the CoE Convention. Moreover, the USA is one of the countries that have ratified the CoE Convention which came into force in 2006. Nevertheless, other factors may have also contributed to this, including the fact that the Internet itself was started and developed in the USA.

Australia and the UK are largely aligned with Articles 2 to 11 of the CoE Convention. This may correspond clearly to the fact that the Cybercrime Act 2001 of Australia is developed based on the Computer Misuse Act 1990 of the UK. Yet, both Acts focus mainly on making illegal the offences against the confidentiality, integrity and the availability of computer data and systems. Section 477.1 of the Cybercrime Act 2001 of Australia and Section 2 of the Computer Misuse Act 1990 of the UK make illegal the unauthorized use of a computer system to commit any of the offences listed under their legislation. These two sections work as an umbrella to make illegal any misuse of computers, even if it is not directed to damage computer data and systems.

The findings show that the UAE is the country least aligned with the CoE Convention. Certain factors may contribute to this finding. The UAE Federal Law No 2 on the Prevention of Information Technology Crimes was only enacted in 2006. Also, on 16 December 2009, the UAE Minister of Justice, Dr Hadef Al Daheri, noted that the UAE Government was setting up a new Department under their Federal Courts to combat cybercrime [46]. The intention of the department was to draft new laws and regulations concerning cybercrime, and set plans for prevention mechanisms and

Table 2. Summary of Australia, UAE, UK and US legislation corresponding to the CoE Convention

CoE Convention	Australia	UAE	UK	USA
Article 2 - Illegal access	Cybercrime Act 2001, Criminal Code Act 1995 (Cth): Section 478.1	UAE Federal Law No 2 of 2006: Article 2	Computer Misuse Act 1990: Section 1	Computer Fraud and Abuse Act, U.S. Code Title 18 Section 1030 (a) (1) – (5)
Article 3 - Illegal interception	Telecommunications (Interception and Access) Act 1979 (Cth): Subsection 7 (1)	UAE Federal Law No 2 of 2006: Article 8	Regulation of Investigatory Powers Act 2000 (RIPA)	U.S. Code Title 18 Sections 2510-2522, Wire and Electronic Communications Interception and Interception of Oral Communications
Article 4 - Data interference	Cybercrime Act 2001, Criminal Code Act 1995 (Cth): Sections 477.2 and 478.2	UAE Federal Law No 2 of 2006: Articles 2 and 6	Computer Misuse Act 1990: Section 3, Data Protection Act 1998	Computer Fraud and Abuse Act, U.S. Code Title 18 Section 1030 (a)(5)
Article 5 - System interference	Cybercrime Act 2001, Criminal Code Act 1995 (Cth): Sections 477.3 and 474.14	UAE Federal Law No 2 of 2006: Article 5	Computer Misuse Act 1990: Section 3	Computer Fraud and Abuse Act, U.S. Code Title 18 Section 1030 (a)(5)
Article 6 - Misuse of devices	Cybercrime Act 2001, Criminal Code Act 1995 (Cth): Sections 478.3 and 478.4		Computer Misuse Act of 1990: Section 3A	Computer Fraud and Abuse Act, U.S. Code Title 18 Sections 1029, 1030 (a)(5)(A) and 2512
Article 7 - Computer-related forgery	Criminal Code Act 1995 (Cth): Div 144, Div 145 and Div 477: Section 477.1	UAE Federal Law No 2 of 2006: Articles 4, 7 and 10	Computer Misuse Act 1990: Section 2, Forgery and Counterfeiting Act 1981	Computer Fraud and Abuse Act, U.S. Code Title 18 Sections 1029, 1037 and 1028, Chapter 25
Article 8 - Computer-related fraud	Criminal Code Act 1995 (Cth): Div 134, Div 135, and Div 477: Section 477.1	UAE Federal Law No 2 of 2006: Articles 10 and 11	Computer Misuse Act 1990: Section 2, Fraud Act 2006: Sections 6 and 7	Computer Fraud and Abuse Act, U.S. Code Title 18 Sections 1029, 1030 (a)(4) and 1343
Article 9 - Offences related to child pornography	Criminal Code Act 1995 (Cth): Sections 474.19 and 474.20, Customs Act 1901 (Cth): Section 233BAB	UAE Federal Law No 2 of 2006: Articles 12 and 13	Protection of Children Act 1978, Sexual Offenses Act 2003, Criminal Justice Act 1988: Sections 160 and 161	Sexual Exploitation of Children, U.S. Code Title 18 Sections 2251, 2252 and 2252A
Article 10 - Offences related to infringements of copyright and related rights	Copyright Act 1968 (Cth)	UAE Federal Law No 7 of 2002 regarding Copyright and Related Rights	Copyright, Design and Patents Act 1988	U.S. Code Title 18 Section 2319, 1030, and 1029 and Title 17: Section 506
Article 11 - Attempt and adding or abetting	Criminal Code Act 1995 (Cth): Sections 478.3 and 478.4	UAE Federal Law No 2 of 2006: Article 23	Computer Misuse Act 1990: Section 2	U.S. Code Title 18 Section 1030 (b)

Table 3. Comparison of penalties[2] for committing computer-related offences identified by the CoE Convention

CoE Convention	Australia	UAE	UK	USA
Article 2 - Illegal access	two years imprisonment	fine and/or at least one year imprisonment	fine and/or up to two years imprisonment	fine and/or up to two years imprisonment
Article 3 - Illegal interception	two years imprisonment	fine and/or imprisonment	fine and/or up to two years imprisonment	fine and/or up to five years imprisonment
Article 4 - Data interference	imprisonment for up to ten years (under s. 477.2)	fine and/or imprisonment	fine and/or up to ten years imprisonment	fine and/or up to ten years imprisonment
Article 5 - System interference	ten years imprisonment	fine and/or imprisonment	fine and/or up to ten years imprisonment	fine and/or up to ten years imprisonment
Article 6 - Misuse of devices	three years imprisonment (under s. 478.4)		fine and/or up to two years imprisonment	fine and/or up to five years imprisonment
Article 7 - Computer-related forgery	imprisonment for up to ten years (under Div 145)	fine and/or at least one year imprisonment	up to five years imprisonment	fine and/or up to fifteen years imprisonment
Article 8 - Computer-related fraud	imprisonment for up to ten years	fine and/or at least one year imprisonment	fine and/or up to ten years imprisonment	fine and/or up to twenty years imprisonment
Article 9 - Offences related to child pornography	imprisonment for up to ten years (under s. 474.19 or s. 474.20)	fine and/or at least five years imprisonment	Imprisonment for up to fourteen years	fine and/or up to thirty years imprisonment
Article 10 - Offences related to infringements of copyright and related rights	fine and/or imprisonment	fine and/or imprisonment	fine and/or up to ten years imprisonment	fine and/or up to ten years imprisonment
Article 11 - Attempt and adding or abetting	three years imprisonment (under s. 478.3 and s. 478.4)	fine and/or imprisonment	fine and/or imprisonment	fine and/or imprisonment

[2] The penalties here depend mainly on violating one section or article of the computer crime or cybercrime law, and accordingly, it could be vary and higher if the committed offence was a second or third offence, not the first committed offence of this type. For instance, violating section 1030 (a)(5) of the U.S. Code is punished by a fine and/or a maximum of ten years imprisonment if it was as a first offence, but if it was as a second offence, the punishment could be up to twenty years imprisonment.

Table 4. Alignment with the CoE Provisions

CoE Convention	Australia	UAE	UK	USA
Article 2 – Illegal access	√	√	√	√
Article 3 – Illegal interception				√
Article 4 – Data interference	√	√	√	√
Article 5 – System interference	√		√	√
Article 6 – Misuse of Devices				√
Article 7 – Computer-related forgery	√		√	√
Article 8 – Computer-related fraud				√
Article 9 – Offences related to child pornography	√	√	√	√
Article 10 – Offences related to infringements of copyright and related rights	√	√	√	√
Article 11 – Attempt and adding or abetting	√		√	√

coordination with law enforcement agencies. Also, we need to consider that cultural factors are an important determinant of a country's regulations. The UAE culture is in many ways significantly different from the culture in Australia, the UK and the USA, as we determined in a separate work addressing cultural influences on national anti-money laundering legislation [47].

Furthermore, our findings indicate that one of the main reasons behind the UAE low alignment with the CoE Convention is the lack of some important conditions for the offences listed under its Law. Most of the UAE Articles do not require the offence to be committed intentionally and without right. These are two important conditions, especially when dealing with cybercrime. While it is not difficult to prove that an offence is committed without right, it is, in practice, difficult and challenging to confirm that the offence was committed intentionally. Articles 2 to11 of the CoE Convention require the offence to be committed 'intentionally', 'wilfully', in Article 10, for criminal liability to apply. Therefore, there is a need to understand the importance of inserting the condition 'intentionally' within the legislation, something which in principle will therefore allow the 'Trojan Horse' defence.

In summary, the above indicates that the UAE legislation is required to be updated. This is but one example of argument in support of the International Telecommunication Union (ITU) 2009 plea for international harmonization [48]: "The lack of a globally harmonized legal framework with respect to cyber criminal activities has become an issue requiring the urgent attention of all nations". While there has been some progress on the legislative front, most notably as a result of the CoE Convention, nonetheless as recently as April 2010 we see a proposal for a global cybercrime treaty rejected at the UN. It seems very clear that there is a need for progress on this front and that to have a global convention on cybercrime, the UN, as an international organization, should take a main role in such a convention and that the CoE Convention which has identified a comprehensive set of computer offences, should be used as a starting point. We argue that this aim must be pursued and that to assist in achieving the aim a six step strategy is required, involving and based on regional participation (this is reminiscent of how Financial Action Task Force (FATF)[3] regional bodies have

[3] The FATF was established in 1989 by the G7 in response to increased concern about money laundering. It develops and promotes policies on AML/CFT; and examines and evaluates its members' AML/CFT approaches (`http://www.fatf-gafi.org`).

cooperated with the international FATF to achieve anti-money laundering/combating financing of terrorism (AML/CFT) aims [40]):

1. identify the main player (the UN) and contributing international organizations (e,g., ITU, CoE, Interpol, G8)
2. identify the sub-players world-wide (regional bodies)
3. identify the relationships between the various participants
4. develop timetables for regional bodies to negotiate and report back to UN on CoE and ITU cybercrime initiatives
5. develop timetables for contributing international organizations to negotiate and report back on CoE and ITU initiatives
6. reconciliation at UN level followed by further cycles of reporting and feedback between participating bodies (essentially re-iteration of steps iv/, v/ and vi/)

5 Australia and the UAE - The Fight against Cybercrime

As part of our studies into how the fight against cybercrime is proceeding internationally, we have analysed the law enforcement procedures employed to combat computer crime, and the legal context in which this occurs, in the state of Queensland in Australia and in the Emirate of Abu Dhabi in the UAE. We have studied the approaches used by the Queensland Police Service (QPS) in Australia and by the Abu Dhabi Police service (ADP) in the UAE to fight cybercrime.

There are two reasons for choosing the ADP to participate in this research project. Firstly, the ADP is funding the project and secondly, the researcher has approval to access and conduct this research in ADP. There are also two reasons for choosing QPS to participate in this research project. Firstly, the research project is located in Queensland and secondly, the researcher, through the cooperation between the QPS and the ADP, has approval to conduct this research. Additionally, we had obtained ethics clearance from the Queensland University of Technology ethics committee to conduct this research.

In order to achieve the objectives, we were given access by the respective law enforcement agencies to some relevant departmental sections. Because of the unavailability of documented procedures on how computer crime units in either the QPS or the ADP operate, identifying their procedures has been achieved through the use of questionnaires completed by the officers and by face to face interviews. Analysis of the resulting data focuses in particular on how the procedures and approaches to combat computer crime by these two law enforcement agencies differ and what improvements are predicated and the nature of the implications for combating computer crime internationally.

Investigating the nature of procedures and guidelines employed by the two agencies using written questionnaires and face to face interviews with the relevant officers has the benefit that it casts light also on the degree to which there is a consistent awareness and interpretation of procedures and guidelines. The study has been conducted in two phases, Phase I and Phase II. Phase I of the study was a pilot study which used a written questionnaire followed by interviews conducted with officers of the two police services, QPS and ADP. The written questionnaire was developed based on the literature review and previous informal meetings with officers from QPS. The Phase I questionnaire questions were developed and structured into three different categories. These categories are:

- Legislation and jurisdiction
- Policy, procedures and resources
- The nature and extent of cybercrime.

Additionally, the second category of *policy, procedures and resources*, included the following themes: policy and procedures; investigation processes; officer experience; resources - technology and computer forensics resources; time to investigate computer crime; education and training; and reporting and statistics.

Then, after analyzing the questionnaire responses, we developed the follow-up interview questions. The questionnaire and interviews were designed to identify how the two law enforcement agencies investigate computer crime, their awareness of the relevant legislation, and their awareness of agency procedures and guidelines for investigating computer-related crime. Phase I found that responses in some areas required further clarification due to issues of unclear and inconsistent responses.

Phase II included performing follow-up in-depth studies using a second written questionnaire and a second set of interviews. This second questionnaire was developed based on the results of Phase I and in line with the research objective. It intended to clarify several responses in some areas that required further clarification due to issues of unclear and inconsistent responses. It also intended to answer additional questions related to computer crime such as jurisdictions, statistics and search warrants.

Our analysis of the data we obtained shows that the ADP and QPS approaches have a number of similar challenges and issues. There are some important issues that continue to create problems for the law enforcement agencies such as sufficient resources, coping internationally with computer crime legislation that differs between countries, and cooperation and communication problems between countries.

This study has also highlighted the importance of having comprehensive documented procedures and guidelines for combating cybercrime. There is a need for formal policy, procedures and guidelines documents regarding the investigation of computer crime. The study also highlights the importance of providing education and training for staff to keep them updated with emerging forms of crime. In summary, we identified the following areas where improvement is mainly needed:

1. availability of formal policy, procedures and guidelines documents
2. resourcing in terms of personnel
3. reporting and recording of cybercrime as distinct from other forms of crime.

6 Conclusions and Future Work

As mentioned earlier, the ITU (2009) notes: “The lack of a globally harmonized legal framework with respect to cyber criminal activities has become an issue requiring the urgent attention of all nations”. This may underestimate the criticality of the problem. Since WW II the world has faced a number of critical global problems. Starvation and genocide, the threat of nuclear war, and - more recently - terrorism, the global financial crisis, and climate change. These problems have required nations around the world to cooperate in pursuit of the common good. The world must recognize that cybercrime is potentially a problem whose seriousness is comparable to that of some of the above given the reliance of government and industry and commerce on the Internet. Indeed, cybercrime clearly contributes to and makes worse some of those

problems, something recognized by the FATF whose efforts have been described earlier. Through the Internet we have created a virtual world that is universally accessible and transnational. It is as a result regulated in a largely ad hoc manner which makes it a rich environment for criminal behaviour. We have created this international virtual world for our convenience but have neglected to design and implement its proper governance. Our paper describes work we have done which we believe can in a small way assist in developing that governance.

We have investigated and analysed some of the issues surrounding disparate definitions and taxonomies of cybercrime and developed a refined and extended taxonomy of cybercrime based upon the dual characteristics of the role of the computer and the contextual nature of the crime. We have used this refined extended taxonomy to analyse a number of iconic cybercrime cases in order to demonstrate its applicability and propose its adoption internationally. We have explored the influence of the CoE Convention internationally by analyzing how the USA, the UK, Australia and the UAE conform to the Convention. These four countries represent a spectrum of development and culture and our results show not surprisingly that more needs to be done in order to address the issue identified by the ITU. We believe a regional approach as we describe in Section 4 is required to progress activities on this front. As part of our analysis of how the fight against cybercrime is proceeding globally, the paper concludes with a comparison of the approaches used by the QPS in Australia and by the ADP in the UAE to fight cybercrime. The analysis shows that resourcing is a problem, and so too are the availability of formal policy, procedures and guidelines documents and the reporting of cybercrime.

Two directions we believe need to be pursued in addition to the above are the detailed evaluation of conformance of national cybercrime legislation with the CoE Convention on Cybercrime, and further research into the comprehensive reporting of cybercrime at the national level in order to provide regulators and legislators with accurate information on cybercrime trends. The reporting needs to include data regarding all cases, regardless of courtroom outcome, together with the extent of resources involved.

References

1. Grabosky, P., Smith, R.G., Dempsey, G.: Electronic Theft: Unlawful Acquisition in Cyberspace. Cambridge University Press, Cambridge (2001)
2. Grabosky, P.: The Global and Regional Cyber Crime Problem. In: Broadhurst, R.G. (ed.) Proceedings of the Asia Cyber Crime Summit, pp. 22–42. Centre for Criminology, The University of Hong Kong, Hong Kong (2001)
3. Furnell, S.M.: The Problem of Categorising Cybercrime and Cybercriminals. In: 2nd Australian Information Warfare and Security Conference, Perth, Australia, pp. 29–36 (2001)
4. United Nations (UN). International Review of Criminal Policy - United Nations manual on the prevention and control of computer-related crime (1999), http://www.uncjin.org/8th.pdf (cited December 6, 2006)
5. G8 Government/Industry Conference on High-Tech Crime. Report of Workshop 3: Threat assessment and prevention. G8 Government/Industry Conference on High-Tech Crime (2001), http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html (cited March 6, 2007)

6. Krone, T.: High Tech Crime Brief: Concepts and terms (2005), http://www.aic.gov.au/publications/htcb/htcb001.pdf (cited February 1, 2007)
7. Kelly, J.X.: Cybercrime - High tech crime (2002), http://www.jisclegal.ac.uk/cybercrime/Archived_cybercrime.htm (cited March 1, 2007)
8. Gordon, S., Ford, R.: On the Definition and Classification of Cybercrime. Journal of Computer Virology 2(1), 13–20 (2006)
9. Broadhurst, R., Grabosky, P. (eds.): Cyber-crime: The challenge in Asia, p. 434. Hong Kong University Press, Hong Kong (2005)
10. Smith, R.G., Grabosky, P., Urbas, G.: Cyber Criminals on Trial, p. 262. Cambridge University Press, Melbourne (2004)
11. Pokar, F.: New Challenges for International Rules Against Cyber-crime. European Journal on Criminal Policy and Research 10(1), 27–37 (2004)
12. Foreign Affairs and International Trade Canada. Cyber Crime, August 16 (2004), http://www.dfait-maeci.gc.ca/internationalcrime/cybercrime-en.asp (cited December 5, 2006)
13. Cybercitizenship. What is Cyber Crime? (2008), http://cybercitizenship.org/crime/crime.html (cited February 19, 2008)
14. Symantec Corporation. What is Cybercrime? (2007), http://www.symantec.com/avcenter/cybercrime/index_page2.html (cited February 5, 2007)
15. Kshetri, N.: The Simple Economics of Cybercrimes. IEEE Security & Privacy 4(1), 33–39 (2006)
16. Wall, D.S.: Cybercrimes: New wine, no bottles? In: Davies, P., Francis, P., Jupp, V. (eds.) Invisible Crimes: Their Victims and their Regulation. Macmillan, London (1999)
17. Grabosky, P.N.: Virtual Criminality: Old Wine in New Bottles? Social & Legal Studies 10(2), 243–249 (2001)
18. Council of Europe. Convention on Cybercrime (2001), http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (cited February 10, 2009)
19. Computer Crime and Intellectual Property Section Criminal Division at U.S. Department of Justice. Prosecuting computer crimes (2007)
20. UK Metropolitan Police Service (MPS). Progress of MPS E-crime Strategy (2007), http://www.mpa.gov.uk/print/committees/mpa/2007/070125/10.htm (cited January 10, 2008)
21. Secretariat of the Parliamentary Joint Committee on the Australian Crime Commission. Cybercrime (2004), http://www.aph.gov.au/senate/committee/acc_ctte/completed_inquiries/2002-04/cybercrime/report/report.pdf (cited January 15, 2008)
22. Brenner, S.W.: U.S. Cybercrime Law: Defining offences. Information Systems Frontiers 6(2), 115–132 (2004)
23. Sukhai, N.B.: Hacking and Cybercrime. In: Proceedings of the 1st Annual Conference on Information Security Curriculum Development, I.s.c. development, Editor, pp. 128–132. ACM Press, Kennesaw (2004)
24. Koenig, D.: Investigation of Cybercrime and Technology-related Crime (2002), http://www.neiassociates.org/cybercrime.htm (cited June 25, 2008)

25. Wilson, C.: Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and policy issues for congress (2008), http://fas.org/sgp/crs/terror/RL32114.pdf (cited June 26, 2008)
26. Lewis, B.C.: Preventing of Computer Crime Amidst International Anarchy (2004), http://goliath.ecnext.com/coms2/summary_0199-3456285_ITM (cited November 17, 2008)
27. Australian High Tech Crime Centre (AHTCC): Fighting the Invisible. Platypus Magazine: Journal of the Australian Federal Police 80, 4–6 (2003), http://www.afp.gov.au/~/media/afp/pdf/f/fighting-the-invisible.ashx
28. Urbas, G., Choo, K.-K.R.: Resources Materials on Technology-enabled Crime, No. 28 (2008), http://www.aic.gov.au/publications/tbp/tbp028/tbp028.pdf (cited November 16, 2008)
29. Thomas, D.: An Uncertain World. The British Computer Society 48(5), 12–13 (2006)
30. Kanellis, P., et al. (eds.): Digital Crime and Forensic Science in Cyberspace. Idea Group Inc., London (2006)
31. Chakrabarti, A., Manimaran, G.: Internet Infrastructure Security: A taxonomy. IEEE Network 16(6), 13–21 (2002)
32. Krone, T.: High Tech Crime Brief: Hacking motives (2005), http://www.aic.gov.au/publications/htcb/htcb006.html (cited February 12, 2007)
33. Keyser, M.: The Council of Europe Convention on Cybercrime. Transnational Law and Policy Journal 12(2), 287–326 (2003)
34. Brenner, S.W.: Defining Cybercrime: A review of the state and federal law. In: Clifford, R.D. (ed.) Cybercrime: The Investigation, Prosecution and Defence of a Computer-Related Crime, pp. 12–40. Carolina Academic Press, North Carolina (2006)
35. Coleman, K.: Cyber Terrorism (2003), http://www.directionsmag.com/article.php?article_id=432&trv=1 (cited February 10, 2009)
36. The UK Parliament Office of Science and Technology. Computer crime (2006), http://www.parliament.uk/documents/upload/postpn271.pdf (cited March 1, 2007)
37. Markoff, J.: Computer Intruder is put on Probation and Fined $10,000 (1990), http://query.nytimes.com/gst/fullpage.html?res=9C0CE1D71038F936A35756C0A966958260 (cited October 7, 2008)
38. Wyld, B.: Cyberterrorism: Fear factor (2004), http://www.crime-research.org/analytics/501/ (cited October 7, 2008)
39. CIO Asia. A Hacker Story (2005), http://www.crime-research.org/articles/hacker0405/ (cited May 28, 2008)
40. Attfield, P.: United States v Gorshkov Detailed Forensics and Case Study: Expert witness perspective, pp. 3–24. IEEE Computer Society, Los Alamitos (2005)
41. Berghel, H.: Fungible Credentials and Next-generation Fraud. Communications of the ACM 49(12), 15–19 (2006)
42. Ninemsn. Cop's Child Porn Case Delayed to Friday (2008), http://news.ninemsn.com.au/article.aspx?id=575167 (cited June 6, 2008)

43. Grow, B., Bush, J.: Hacker Hunters (2005), http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm (cited October 21, 2006)
44. SCAMwatch. The Holiday Prize Which Nearly Cost Nicole Thousands of Dollars (2008), http://www.scamwatch.gov.au/content/index.phtml/itemId/699124 (cited October 17, 2008)
45. U.S. Department of Justice. Fourth defendant in massive Internet scam pleads guilty to fraud and money laundering charges (2004), http://www.usdoj.gov/criminal/cybercrime/nordickPlea_triwest.htm (cited November 3, 2008)
46. Gulfnews. New Department to Fight Cyber Crimes (2009), http://gulfnews.com/news/gulf/uae/crime/new-department-to-fight-cyber-crimes-1.554070 (cited December 25, 2009)
47. Alkaabi, A., et al.: A Comparative Analysis of the Extent of Money Laundering in Australia, UAE, UK and the USA. In: Finance and Corporate Governance Conference, Melbourne (2010), http://ssrn.com/abstract=1539843
48. International Telecommunication Union. ITU Toolkit for Cybercrime Legislation (2009) (updated on February 2010), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf (cited November 3, 2009)