Combating Computer Crime: An International Perspective

Ali Obaid Sultan Alkaabi

Bachelor of Computer Science, University of the UAE
Master of Information Technology, University of Southern Queensland

Thesis submitted in accordance with the regulations for the Degree of Doctor of Philosophy

Information Security Institute
Faculty of Science and Technology
Queensland University of Technology

October 2010
Keywords

Computer crime, computer-related crime, cybercrime, high-tech crime, money laundering, anti-money laundering, AML/CFT, culture, legislation, Australia, UAE, UK, USA.
Abstract

Given the serious nature of computer crime, and its global nature and implications, it is clear that there is a crucial need for a common understanding of such criminal activity internationally in order to deal with it effectively. Research into the extent to which legislation, international initiatives, and policy and procedures to combat and investigate computer crime are consistent globally is therefore of enormous importance. The challenge is to study, analyse, and compare the policies and practices of combating computer crime under different jurisdictions in order to identify the extent to which they are consistent with each other and with international guidelines; and the extent of their successes and limitations. The purpose ultimately is to identify areas where improvements are needed and what those improvements should be.

This thesis examines approaches used for combating computer crime, including money laundering, in Australia, the UAE, the UK and the USA, four countries which represent a spectrum of economic development and culture. It does so in the context of the guidelines of international organizations such as the Council of Europe (CoE) and the Financial Action Task Force (FATF). In the case of the UAE, we examine also the cultural influences which differentiate it from the other three countries and which has necessarily been a factor in shaping its approaches for countering money laundering in particular.

The thesis concludes that because of the transnational nature of computer crime there is a need internationally for further harmonisation of approaches for combating computer crime. The specific contributions of the thesis are as follows:

- Developing a new unified comprehensive taxonomy of computer crime based upon the dual characteristics of the role of the computer and the contextual nature of the crime
- Revealing differences in computer crime legislation in Australia, the UAE, the UK and the USA, and how they correspond to the CoE Convention on
Cybercrime and identifying a new framework to develop harmonised computer crime or cybercrime legislation globally

- Identifying some important issues that continue to create problems for law enforcement agencies such as insufficient resources, coping internationally with computer crime legislation that differs between countries, having comprehensive documented procedures and guidelines for combating computer crime, and reporting and recording of computer crime offences as distinct from other forms of crime

- Completing the most comprehensive study currently available regarding the extent of money laundered in four such developed or fast developing countries

- Identifying that the UK and the USA are the most advanced with regard to anti-money laundering and combating the financing of terrorism (AML/CFT) systems among the four countries based on compliance with the FATF recommendations. In addition, the thesis has identified that local factors have affected how the UAE has implemented its financial and AML/CFT systems and reveals that such local and cultural factors should be taken into account when implementing or evaluating any country’s AML/CFT system.
Dedication

This thesis is dedicated to HH Lt. General Sheikh Saif bin Zayed Al Nahyan, Deputy Prime Minister and Minister of Interior who has inspired, encouraged and supported the UAE students, including myself, to complete our studies overseas.
Contents

Keywords .......................................................................................................................... i
Abstract ............................................................................................................................. iii
Dedication ........................................................................................................................... v
Contents .............................................................................................................................. vii
List of Figures ..................................................................................................................... xi
List of Tables ....................................................................................................................... xiii
List of Abbreviations .......................................................................................................... xv
Statement of Original Authorship ....................................................................................... xvii
Previously Published Material .......................................................................................... xix
Acknowledgements ............................................................................................................ xxi

Chapter 1 Introduction ......................................................................................................... 1
  1.1 Scope and Significance of Research, and Summary of Approach ................................. 2
  1.1.1 Scope ......................................................................................................................... 2
  1.1.2 Significance ............................................................................................................... 3
  1.1.3 Summary of Approach ............................................................................................. 5
  1.2 Research Objectives and Questions ............................................................................. 5
  1.3 Contributions ............................................................................................................... 9
  1.4 Conclusion .................................................................................................................... 11

Chapter 2 Computer Crime: Past and Present .................................................................... 13
  2.1 Computer Crime ........................................................................................................... 13
  2.1.1 Definitions ............................................................................................................... 14
  2.1.2 Taxonomies ............................................................................................................. 17
  2.1.3 Global Extent of Computer Crime ........................................................................... 21
  2.2 Combating Computer Crime ......................................................................................... 22
  2.2.1 International Initiatives to Combat Computer Crime ................................................. 23
  2.2.2 Computer Crime and Cybercrime Legislation ......................................................... 28
  2.2.3 Government Initiatives to Combat Computer Crime .............................................. 33
  2.2.4 Law Enforcement Approaches to Combat Computer Crime .................................. 38
  2.3 Combating Money Laundering ...................................................................................... 50
  2.3.1 Money Laundering ................................................................................................... 51
  2.3.2 International Approaches for Combating Money Laundering ................................. 53
  2.3.3 National Approaches for Combating Money Laundering ....................................... 58
  2.4 Limitations of the Existing Approaches ..................................................................... 65
  2.4.1 Legislation and Jurisdiction ...................................................................................... 65
  2.4.2 Policy and Procedures ............................................................................................... 67
  2.4.3 Technology and Staff Resources .............................................................................. 67
  2.4.4 Computer Crime and Statistics ............................................................................... 68
  2.4.5 Summary .................................................................................................................. 69
  2.5 Research Methodology ................................................................................................. 70
  2.6 Conclusion .................................................................................................................... 75
Chapter 3 The Nature of Computer Crime and the Harmonisation of Computer Crime Legislation ........................................................................................................... 77
  3.1 A Model for Classifying Computer Crime ........................................................................................................... 79
    3.1.1 The Need for a Consistent Taxonomy of Computer Crime .............................................................................. 80
    3.1.2 The Refined Type I/II Model - Refining the Role I and Role II Classification of Computer Crime .................. 81
    3.1.3 The Extended Refined Model – Extended with Contextual Features ................................................................. 85
    3.1.4 A Universal Classification Code for Computer Crime ......................................................................................... 89
    3.1.5 The CoE Convention and the Refined (Type/Sub-type) Computer Crime Classification ................................... 91
  3.2 Cybercrime Legislation Alignment with the CoE Convention on Cybercrime ................................................. 92
  3.3 Proposal to Develop Harmonised Cybercrime Legislation Globally ............................................................ 97
    3.3.1 A New Strategy ............................................................................................................................................... 97
    3.3.2 Summary .................................................................................................................................................... 104
  3.4 Conclusion ....................................................................................................................................................... 104

Chapter 4 Case Study: Combating Computer Crime in Australia and the UAE ................................................. 107
  4.1 Methodology ..................................................................................................................................................... 108
    4.1.1 Overall Methodology .................................................................................................................................... 109
    4.1.2 Phase I – Pilot Study ..................................................................................................................................... 111
    4.1.3 Phase II – Further Study ................................................................................................................................ 112
  4.2 Cross-Case Findings – QPS vs. ADP .................................................................................................................. 113
    4.2.1 Proposition 1 – Legislation and Jurisdiction .................................................................................................. 113
    4.2.2 Proposition 2 – Policy, Procedures and Resources ......................................................................................... 114
    4.2.3 Proposition 3 – Nature and Extent of Computer Crime .................................................................................. 121
  4.3 Discussion ....................................................................................................................................................... 124
    4.3.1 Summary of Findings ................................................................................................................................... 124
    4.3.2 Needed Improvements and Challenges ........................................................................................................ 126
  4.4 Conclusion ....................................................................................................................................................... 127

Chapter 5 The Extent of Money Laundering ......................................................................................................... 131
  5.1 Money Laundering Estimates .......................................................................................................................... 132
  5.2 Anti-money Laundering Statistics: Suspicious Activity Reports (SARs) and Cases, Prosecutions and Convictions ........................................................................................................ 140
    5.2.1 Reporting Requirements and SARs ................................................................................................................ 140
    5.2.2 Anti-money Laundering Statistics: Cases, Prosecutions and Convictions ...................................................... 145
  5.3 Discussion ....................................................................................................................................................... 147
  5.4 Conclusion ....................................................................................................................................................... 149

Chapter 6 Money Laundering and FATF Compliance by Australia, the UAE, the UK and the USA ................................................................. 151
  6.1 Compliance with the FATF 40+9 Recommendations ............................................................................................ 153
    6.1.1 Compliance with the FATF 40 Recommendations .......................................................................................... 155
    6.1.2 Compliance with the FATF 9 Special Recommendations ........................................................................... 160
    6.1.3 Implications of Non-compliance with FATF .................................................................................................. 160
  6.2 Discussion: Factors Affecting Compliance ........................................................................................................... 163
    6.2.1 Religious and Cultural Factors ...................................................................................................................... 163
    6.2.2 Socio-economic and Financial Factors ........................................................................................................ 167
    6.2.3 Summary .................................................................................................................................................... 169
  6.3 Conclusion ....................................................................................................................................................... 169

Chapter 7 Conclusion and Future Work ............................................................................................................. 171
  7.1 Summary of Contributions .................................................................................................................................. 172
Appendix A: Detailed Analysis of Computer Crime Case Studies ........................................................................................................199
Appendix B: CoE Convention on Cybercrime .................................................................................................................................205
  Appendix B.1: Articles 2 to 11 of the CoE Convention on Cybercrime ..........................................................................................205
  Appendix B.2: Detailed Analysis of the CoE Convention on Cybercrime .....................................................................................211
  Appendix B.3: Detailed Analysis of the Existence and Alignment of Computer Crime or Cybercrime Legislation Relating to the CoE Convention in Australia, the UAE, the UK and the USA .........................................................................................220
Appendix C: Questionnaires and Interview Questions – Phase I ........................................................................................................245
  Appendix C.1: Questionnaires Questions – QPS and ADP ...........................................................................................................245
  Appendix C.2: QPS – Interview Questions ........................................................................................................258
  Appendix C.3: ADP – Interview Questions ........................................................................................................265
Appendix D: Questionnaires and Interview Questions – Phase II .......................................................................................................267
  Appendix D.1: QPS – Questionnaire Questions ................................................................................................................267
  Appendix D.2: QPS – Interview Questions ................................................................................................................278
  Appendix D.3: ADP – Questionnaire Questions ................................................................................................................285
  Appendix D.4: ADP – Interview Questions ................................................................................................................295
List of Figures

Figure 2.1 Types of high-tech crime classification (Adapted from [44]) ...................................... 18
Figure 2.2 The common types of computer crime according to the UN (Adapted from [49]) .... 19
Figure 2.3 The CoE taxonomy of cybercrime offences (Adapted from [20]) .......................... 20
Figure 2.4 The G8 taxonomy of threats (Adapted from [50]) .................................................. 21
Figure 2.5 Example of how the investigation of money laundering works in Australia .......... 62
Figure 3.1 Refined computer crime classification ................................................................. 85
Figure 5.1 Number of SARs per 1,000 of the population in Australia, UAE, the UK and the USA, 1999–2008 ........................................................................................................ 144
Figure 5.2 Number of SARs per unit (billions of dollars) of GDP in Australia, UAE, the UK and the USA, 1999–2008 ......................................................................................... 144
List of Tables

Table 2.1 The main legislation for combating computer crime and cybercrime used in Australia, the UAE, the UK and the USA ................................................................. 33
Table 2.2 Type of computer crime and the appropriate federal investigative agencies where the crime should be reported (From [107]) .............................................................................................................................................. 49
Table 3.1 Discussion of some computer crime case studies ................................................. 87
Table 3.2 Characteristics of some computer crime case studies ......................................... 88
Table 3.3 Universal code for the types of computer crime .................................................. 90
Table 3.4 Mapping the CoE Convention to the proposed computer crime classification ....... 91
Table 3.5 Summary of Australia, the UAE, the UK and the USA legislation corresponding to the CoE Convention .......................................................................................... 94
Table 3.6 Comparison of penalties for committing computer-related offences identified by the CoE Convention ......................................................................................... 95
Table 3.7 Alignment with Articles 2 to 11 of the CoE Convention ..................................... 96
Table 4.1 Cross case comparison for the first proposition .................................................. 114
Table 4.2 The ADP investigation processes .................................................................... 117
Table 4.3 The QPS investigation processes .................................................................... 117
Table 4.4 Identify how the investigation process of ADP and QPS related to the five investigation stages ................................................................................................. 118
Table 4.5 Type of courses used by QPS and ADP to upgrade the skills of the investigators .... 120
Table 4.6 Type of outcome reports used by QPS and ADP ................................................. 121
Table 4.7 Type of computer crime investigated by QPS and ADP participants .................... 123
Table 4.8 Type of crime and number of cases investigated by QPS and ADP participants over 12 months from the date of the Phase II questionnaire (March 2008 for ADP, April 2008 for QPS) .................................................................................................................. 124
Table 4.9 Challenges and issues that face QPS and ADP and what initiatives and activities do they use to manage them ..................................................................................... 128
Table 5.1 Estimations of the extent of money laundering in the world annually .................. 133
Table 5.2 Estimations of the extent of money laundering in Australia, the UAE, the UK and the USA, 1999–2008, based on the GDP .............................................................................. 135
Table 5.3 Estimations of the amount of laundered money in Australia ............................... 137
Table 5.4 Estimation of the amount of laundered money in the UAE ................................. 138
Table 5.5 Estimations of the amount of laundered money in the USA ............................... 138
Table 5.6 Estimations of the amount of laundered money in the UK ................................. 139
Table 5.7 SARs identification criteria in Australia, UAE, the UK and the USA based on the FATF criteria ................................................................................................................. 142
Table 5.8  SARs received in Australia, the UAE, the UK and the USA, 1999–2008 .................. 143
Table 5.9  Money laundering prosecutions and convictions in the Australia, the UAE, the UK and the USA ................................................................. 146
Table 5.10  Money laundering prosecutions and convictions in the UK, 1999–2007 ............. 146
Table 6.1  Years of evaluations of AML systems of Australia, the UAE, the UK and the USA in relation to the FATF recommendations ................................................. 153
Table 6.2  The FATF core and key recommendations on AML/CFT ................................. 154
Table 6.3  Comparison of compliance with the FATF 40 recommendations between the AML systems used in Australia, the UAE, the UK and the USA ........................................ 158
Table 6.4  Summary of compliance with the FATF 40 Recommendations on AML ............ 159
Table 6.5  Summary of compliance with the FATF 9 special recommendations on CFT .......... 160
Table 6.6  The population and GDP of Australia, UAE, the UK and the USA, 1999–2008 ........ 160
Table B1  CoE provisions for illegal access and the related provisions and alignment from Australia, the UAE, the UK and the USA .................................................. 222
Table B2  CoE provisions on illegal interception and the related provisions and alignment from Australia, the UAE, the UK and the USA .................................................. 224
Table B3  CoE provisions for data interference and the related provisions and alignment from Australia, the UAE, the UK and the USA .................................................. 227
Table B4  CoE provisions for system interference and the related provisions and alignment from Australia, the UAE, the UK and the USA .................................................. 230
Table B5  CoE provisions for misuse of devices and the related provisions and alignment from Australia, the UAE, the UK and the USA .................................................. 233
Table B6  CoE provisions for computer-related forgery and the related provisions and alignment from Australia, the UAE, the UK and the USA ............................................. 235
Table B7  CoE provisions for computer-related fraud and the related provisions and alignment from Australia, the UAE, the UK and the USA ............................................... 238
Table B8  CoE provisions for offences related to child pornography and the related provisions and alignment from Australia, the UAE, the UK and the USA ....................... 241
Table B9  CoE provisions for computer-related forgery and the related provisions and alignment from Australia, the UAE, the UK and the USA ............................................. 242
Table B10  CoE provisions for aiding, abetting or attempting the commission of any of the offences established under Articles 2–10 and the related provisions and alignment from Australia, the UAE, the UK and the USA ....................... 244
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACC</td>
<td>Australian Crime Commission</td>
</tr>
<tr>
<td>ACPO</td>
<td>Association of Chief Police Officers</td>
</tr>
<tr>
<td>ACPR</td>
<td>Australian Centre for Police Research</td>
</tr>
<tr>
<td>ADP</td>
<td>Abu Dhabi Police</td>
</tr>
<tr>
<td>AHTCC</td>
<td>Australian High-Tech Crime Centre</td>
</tr>
<tr>
<td>AML</td>
<td>Anti-money Laundering</td>
</tr>
<tr>
<td>AML/CFT</td>
<td>Anti-money Laundering and Combating the Financing of Terrorism</td>
</tr>
<tr>
<td>AMLSCU</td>
<td>Anti-Money Laundering and Suspicious Cases Unit</td>
</tr>
<tr>
<td>ATO</td>
<td>Australian Taxation Office</td>
</tr>
<tr>
<td>AUSTRAC</td>
<td>Australian Transaction Reports Analysis Centre</td>
</tr>
<tr>
<td>CCIU</td>
<td>Computer Crime Investigation Unit</td>
</tr>
<tr>
<td>CFT</td>
<td>Combating the Financing of Terrorism</td>
</tr>
<tr>
<td>CFTT</td>
<td>Computer Forensics Tool Testing (CFTT)</td>
</tr>
<tr>
<td>CoE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FCEU</td>
<td>Forensic Computer Examination Unit</td>
</tr>
<tr>
<td>FinCEN</td>
<td>Financial Enforcement Network</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit</td>
</tr>
<tr>
<td>FLETC</td>
<td>Federal Law Enforcement Training Center</td>
</tr>
<tr>
<td>FTR Act</td>
<td>Financial Transaction Reports Act 1988</td>
</tr>
<tr>
<td>GCC</td>
<td>Gulf Co-operation Council</td>
</tr>
<tr>
<td>GPML</td>
<td>Global Programme against Money Laundering</td>
</tr>
<tr>
<td>G7</td>
<td>Group of Seven</td>
</tr>
<tr>
<td>G8</td>
<td>Group of Eight</td>
</tr>
<tr>
<td>IC3</td>
<td>Internet Crime Complaint Center</td>
</tr>
<tr>
<td>IDCU</td>
<td>Identity Crime Unit</td>
</tr>
<tr>
<td>IMF</td>
<td>International Monetary Fund</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Name</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunications Union</td>
</tr>
<tr>
<td>MFIG</td>
<td>Major Fraud Investigation Group</td>
</tr>
<tr>
<td>NCFTA</td>
<td>National Cyber-Forensics and Training Alliance</td>
</tr>
<tr>
<td>NHTCU</td>
<td>National Hi-Tech Crime Unit</td>
</tr>
<tr>
<td>NIJ</td>
<td>National Institute of Justice</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>PoCU</td>
<td>Proceeds of Crime Unit</td>
</tr>
<tr>
<td>QPS</td>
<td>Queensland Police Service</td>
</tr>
<tr>
<td>SARs</td>
<td>Suspicious Activity Reports</td>
</tr>
<tr>
<td>SOCA</td>
<td>Serious Organised Crime Agency</td>
</tr>
<tr>
<td>STRs</td>
<td>Suspicious Transaction Reports</td>
</tr>
<tr>
<td>SWIFT</td>
<td>Society for Worldwide Interbank Financial Telecommunication</td>
</tr>
<tr>
<td>UAE</td>
<td>United Arab Emirates</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UNCAC</td>
<td>UN Convention Against Corruption</td>
</tr>
<tr>
<td>UNODC</td>
<td>United Nations Office on Drugs and Crime</td>
</tr>
<tr>
<td>USA</td>
<td>United States of America</td>
</tr>
</tbody>
</table>
Statement of Original Authorship

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signed: [Signature] Date: 27/10/2010
Previously Published Material

The following papers have been published or presented, and contain material based on the content of this thesis.


Acknowledgements

Praise and thanks be to Allah for his help in accomplishing this work.

It is a pleasure to thank the following individuals and organizations who made this thesis possible.

I would like to express my deep and sincere gratitude to my principal supervisor Professor George Mohay. His encouragement, patience, guidance and support have been of great value to me in order to complete this work. I could not have imagined having a better advisor for my PhD study. Thank you very much George.

Besides my principal supervisor, I would like to thank the rest of my supervision team, Adjunct Professor Adrian McCullagh and Dr Nic Chantler for their encouragement, insightful comments and support. Indeed, Adrian was a valuable addition to my supervision team who provided a great deal of good ideas and suggestions. I would like also to thank Associate Professor Andrew Clark for all his assistance and support during the first two years of my PhD.

Acknowledgement is due to the Abu Dhabi Police, Ministry of Interior, in the United Arab Emirates for sponsoring and supporting my research. I am also very grateful to Major General Nasser Al Nuaimi, Secretary General of the Office of HH the Deputy Prime Minister and Minister of Interior, for supporting my research and also allowing me to conduct part of this research with the Abu Dhabi Police. Additional thanks go to all of the Abu Dhabi Police officers who participated in this work.

I am also very grateful to the Queensland Police Service in Australia for participating in my research. I wish to express my warm and sincere thanks to the Commissioner of Queensland Police Service, Bob Atkinson, for allowing me to conduct part of this research with the Queensland Police Service. I am also very grateful to Detective Superintendent Brian Hay, State Crime Operations Command
- Queensland Police Service, for his understanding, support and providing the resources for conducting this research. Additional thanks go to all of the Queensland Police officers who participated in this work.

I am grateful to a number of people who facilitated the cooperation between the Abu Dhabi Police and Queensland Police and also made this work possible. My thanks go to Dr Glenda Adkins, University of Southern Queensland, Chief Superintendent Steve Hollands and Inspector Mark Wheatley, Queensland Police Service. I am heartily thankful to them.

I would like to thank the Information Security Institute at the Queensland University of Technology for providing the resources and environment for conducting this research. I would like also to thank my colleagues at the Information Security Institute for their support during my research.

I wish to thank my entire extended family for their understanding, support and guidance. I am heartily thankful to my uncle, Obaid Mohd Alkaabi, for his encouragement, guidance and support. Also, and most importantly, I wish to thank my parents, my grandmother, my wife and my daughter, Mouza. Without them I could not have completed this work.

Lastly, I offer my best wishes and regards to all of those who encouraged and supported me in any respect during my research.
In an increasingly globalised and electronic world, the extent of computer-related crime within and across countries is reaching mammoth proportions. The term *computer crime* is synonymous with the term *computer-related crime*, which, in turn, may involve only a stand-alone computer or it may involve cybercrime implying the use or abuse of computer networks, such as the Internet, for criminal activity. 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. Cybercrime is the United States of America (USA) Federal Bureau of Investigation’s (FBI) third top priority [1, 2] and according to the FBI’s estimation, cybercrime in the USA cost industries about US$400 billion in 2004 [3, 4]. The Department of Trade and Industry in the United Kingdom (UK) noted that computer crime increased by 50% over 2004 and 2005 [3]. At the international level, cybercrime is one of Interpol’s top five priorities [5]. Research into how best to combat computer crime is, therefore, of the utmost importance.

This chapter provides a summary of the research problems dealt with in the work presented in this thesis and the objectives of that work. It presents a brief background to the topic of the thesis and its scope, and presents the contributions of the thesis and describes its structure.
1.1 Scope and Significance of Research, and Summary of Approach

1.1.1 Scope

At present, there is a large number of terms used to describe crime involving computers. Such terms include computer related crime [5-7], computer crime [5-8], Internet crime [6, 7], e-crime [6, 7], digital crime [6, 9], high-tech crime [6], online crime [6], electronic crime [6], computer misconduct [10], cybercrime [5-8, 11-15]. The latter has been widely used recently [5-8, 11-15]. Historically, cybercrime has referred to crimes happening specifically over networks, especially the Internet, but that term has gradually become a general synonym for computer crime. Yet another synonym, 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. Likewise, the United Arab Emirates (UAE) Federal Law No (2) of 2006 on The Preventive of Information Technology Crimes [16] provides a very broad meaning for high-tech or cybercrime to include all offences against computer data and systems, computer-related offences, content-related offences and other offences such as those that violate religious beliefs or threaten and violate family principles. In fact, many researchers indicated that the above terms are sometimes used interchangeably to describe the same crimes [7, 17].

Under the Cybercrime Act 2001 of Australia, the term cybercrime refers to crimes that target computer data and systems. The USA Department of Justice, Computer Crime and Intellectual Property Section, defines [18] 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 Symantec Corporation [19] defines cybercrime broadly as "any crime that is committed using a computer or network, or hardware device — the computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime". Under the Council of Europe (CoE) Convention on Cybercrime, the term cybercrime refers to offences against the confidentiality, integrity and availability of computer data.
and systems, computer-related offences, content-related offences and offences related to infringements of copyright and related rights [20].

Summary

The term computer crime is used broadly in the media, by the community at large and by the IT profession to refer to crimes that involve computers — crimes that are computer-related. The related term cybercrime was originally used in a more precise sense to refer to criminal activity using or targeting a global network or information system. The term in its original sense does not apply to computer crimes that involve only a stand-alone computer system, digital device or a closed computer network. In general, it does apply to crimes involving the Internet. This thesis is concerned with computer crimes of both sorts — crimes involving stand-alone computers or devices or networks, and crimes undertaken via the Internet. The global nature and rapid uptake of the Internet has resulted in enormously increased opportunities for cybercrime, criminal activity that uses the Internet for illegal purposes and criminal activity that intends to disrupt the Internet-reliance of organizations and nations. As mentioned, in recent times, there has been a general acceptance of a broader interpretation for the term cybercrime ([19] and [20]), making it synonymous with computer crime and many of the references we cite in this chapter, and elsewhere in the thesis, that refer to cybercrime actually relate to computer crime in the broad sense, viz., including crimes involving stand-alone systems. These terms and others are discussed in more detail in Chapter 2. The thesis mostly uses the two terms computer crime and cybercrime more or less interchangeably, using the latter term in its broad sense, but distinguishing where necessary between criminal activity involving stand-alone systems and criminal activity involving the Internet.

1.1.2 Significance

Combating and investigating computer crime successfully are complex tasks that rely upon adopting best practices in legislation, policy and procedures, and technology and resources. The challenge for this work is to study, analyse and compare the policies and practices of combating computer crime under
different jurisdictions to identify their successes and limitations and improvements needed. Computer crime is today a global activity, and this thesis will establish that there is a major disconnect in how the various jurisdictions have dealt with this relatively new criminal activity and that legislators, owing to various influences, especially cultural influences, have approached anti-money laundering activities in particular differently. Consequently, criminals can take advantage of this and undermine global attempts to combat cybercrime.

The effect of cybercrime on society is huge. The UK National Hi-Tech Crime Unit (NHTCU) estimates the cost of high-tech crime for companies based in UK was at least US$4.61 billion in 2004 [21]. Also, according to the USA Treasury Department, the proceeds from cybercrime have overtaken the proceeds from illegal drug sales netting an estimated US$105 billion in 2004 [22, 23]. Given the serious nature of computer crime and its global nature and implications, it is clear that there is a crucial need for a common understanding of such criminal activity internationally to deal with it effectively. Therefore, research into the extent to which legislation, international initiatives, policy and procedures, and technology to combat and investigate computer crime are consistent globally is, naturally, of enormous importance.

The Internet has enhanced the transfer of information and how the world communicates. Nowadays, many services are available over the Internet such as Internet banking, shopping, auctions, gambling and other services that are increasing in both number and size. This provides an opportunity for the widespread growth of cybercrime through the Internet. Richard Power [24] from the Computer Security Institute says that “as the world moves into cyberspace and as all money flows into cyberspace, crime follows money and you are going to see it there”. However, there are some differences in the approaches of combating computer crime from one jurisdiction to another, and these differences can and sometimes do impede global efforts to combat cybercrime.
1.2.1 Summary of Approach

This research project investigates the approaches for countering computer crime in Australia, the UAE, the UK and the USA, in the context of the guidelines of international organizations, such as the CoE and the Financial Action Task Force (FATF). It does so in order to identify improvements that are needed in combating cybercrime globally. Some aspects of the research have been conducted in cooperation with the Queensland Police Service (QPS) in Australia and the Abu Dhabi Police (ADP) in the UAE. The QPS and the ADP have provided the researcher with assistance during the period of study and this is gratefully acknowledged.

This thesis examines the approaches used for combating computer crime in Australia, the UAE, the UK and the USA, four countries which represent a spectrum of economic development and culture. In the case of the UAE, we also examine the cultural influences that differentiate it from the other three countries and which have necessarily been a factor in shaping its approaches for countering money laundering in particular, an especially insidious and significant form of computer crime. We have selected these four countries for a number of reasons. The UAE has been selected because the funding for this research has been provided by the UAE and because the UAE, while a modern and fast developing economy, is an Islamic jurisdiction and thus, to that extent, distinctly different from the other three countries. Australia is included because the research has been undertaken in Australia. The UK has been selected as a jurisdiction representative of the European Community, and the USA has been selected for a number of reasons, the main one being that, as the world’s largest economy, it needs to be included in any study of this nature.

1.2 Research Objectives and Questions

As indicated above, computer crime poses a significant problem for the global community and cybercrime via the Internet forms the major part of this. The Internet is both a target and a conduit for such activity and its trans-national
character means that combating cybercrime requires concerted international effort.

The objective of this thesis is to examine the extent to which there is a common and effective approach to combating computer crime internationally and the extent to which such efforts are succeeding and improvements are needed. The thesis aims to investigate and compare different jurisdictions from around the world and their approaches to combating computer crime with a view to understanding the effectiveness of their approaches and the factors that have influenced that. As mentioned, the jurisdictions are the following four countries: the USA and the UK, two G8 countries; a smaller, developed country, Australia; and the UAE, which is a fast-developing country with a very different historical culture. The thesis examines the nature of computer crime and the different and sometimes contrasting definitions and taxonomies that are used to classify computer crime and cybercrime, and proposes some elaborations to those. It also reviews and compares the current legislation for combating computer crime and cybercrime used in Australia, the UAE, the UK and the USA with regard to their alignment with the Council of Europe (CoE) Convention on Cybercrime.

Additionally, for the purpose for comparing how law enforcement agencies in two different international jurisdictions investigate computer crime, this research uses a case study-based approach to investigate the approaches used by the Abu Dhabi Police (ADP) in the UAE, and the Queensland Police Service (QPS) in Australia. There are two reasons for choosing the ADP to participate in this research project. First, the ADP is funding the project and second, the researcher has approval to access and conduct this research in the ADP. There are also two reasons for choosing the QPS to participate in this research project. First, the research project is located in Queensland and second, the researcher, through the cooperation between the QPS and the ADP, has approval to conduct this research.

The thesis also focuses on money laundering. Money laundering has been transformed in the past decade or less by the Internet, giving rise to the new term *cyber-laundering*. Lovet (2009) [25] entirely captures the nature of this
transformation when he refers to the Internet as the big cyber-laundering machine. While it is clear that some forms of money laundering do not constitute cybercrime, it is also clear that money laundering implemented via the Internet — cyber-laundering — does. Indeed, in some countries, including the UAE, money laundering that happens over the Internet is specifically criminalised under cybercrime legislation. The International Monetary Fund (IMF) has estimated that the extent of money laundering globally is between 2 to 5% of the world’s gross domestic product [26]. This figure is larger than the GDP of all but a handful of countries and represents correspondingly huge risks to global financial stability and to the financial well-being and stability of many countries. For these reasons, and as previously mentioned, this thesis also focuses on the crime of money laundering and examines both the extent of money laundering in the four selected countries and the extent of their compliance with the important FATF anti-money laundering and countering the financing of terrorism recommendations.

In summary, the overall aim of this research is to identify what improvements are needed in international efforts to combat computer crime and in order to do so, we address the following more specific objectives:

- To review and analyse different definitions and taxonomies of computer crime
- To review and compare the current legislation for combating computer crime and cybercrime used in Australia, the UAE, the UK and the USA and their alignment with the Council of Europe (CoE) Convention on Cybercrime
- To investigate and compare the computer crime combating approaches used by the Queensland Police Service (QPS) in Australia and the Abu Dhabi Police (ADP) in the UAE, two countries representing different international jurisdictions and cultures, as a case study to provide an insight into how such approaches vary internationally
- To study the extent of money laundering in Australia, the UAE, the UK and the USA, in addition to studying how these countries comply with the Financial Action Task Force (FATF) recommendations.
The overall research question for this thesis is:

*Given the serious and global nature of computer crime and taking into account varying cultural differences and influences, is there internationally a sufficient understanding of it and a sufficiently consistent approach for dealing with it effectively, and what improvements are needed?*

Arising from the above, the following specific research questions have been formulated:

**Q1.** To what extent are the current definitions and taxonomies of computer crime and current computer crime or cybercrime legislation appropriate for the effective investigation and prosecution of cybercrime in the international context and what improvements are needed?

To answer this question, we focus on two more specific research questions:

**Q1(a)** To what extent are the current definitions and taxonomies of computer crime appropriate to the accurate and consistent reporting internationally of computer crime and its prosecution and what improvements are needed?

**Q1(b)** To what extent does the computer crime or cybercrime legislation in Australia, the UAE, the UK and the USA differ and to what extent is that legislation in alignment with the Council of Europe (CoE) Convention on Cybercrime and what improvements are needed in this regard?

**Q2.** To what extent are the approaches for combating computer crime in Australia (as represented by the QPS) and the UAE (as represented by the ADP) different and what improvements are needed?

**Q3.** To what extent does the extent of money laundering in Australia, the UAE, the UK and the USA differ and how has it changed over time?

**Q4.** To what extent do the anti-money laundering/combating financing of terrorism regimes in Australia, the UAE, the UK and the USA differ with respect to their compliance with the international Financial Action Task Force (FATF) recommendations and to what extent have local factors, such as cultural and economic factors, affected the UAE’s compliance with these recommendations and what improvements are needed?
1.3 Contributions

This research analyses the approaches used by Australia, the UAE, the UK and the USA for combating computer crime, investigates (i) how their approaches are different and, (ii) the influence of the local factors on how these approaches have been developed and implemented.

The main contribution of the research is the analysis of the approaches used in Australia, the UAE, the UK and the USA for combating computer crime and identification of areas where improvement is needed. In contrast to the other three countries, the UAE was only established in 1971 [27]. The thesis has revealed that local factors, such as recent history, cultural and religious factors, have influenced the development of computer crime approaches in the UAE and have resulted in differences in approach with respect to the other countries that are yet to be reconciled. Such differences between the nations have the potential to compromise global efforts to resolve computer crime and, given the scale of computer crime globally and its progressive increase, such differences are of acute concern.

Chapter 2 provides a detailed literature review on computer crime and the approaches used for combating such crime. It highlights the cybercrime legislation used in Australia, the UAE, the UK and the USA. Chapter 2 also examines national approaches and international initiatives to combat computer crime, including money laundering. It then discusses the limitations of the existing approaches for combating computer crime and the methodology used to conduct this research.

In Chapter 3, the thesis reveals the differences in definitions and taxonomies of computer crime that makes for some inconsistencies in the reporting of such criminal activity. It proposes a unified comprehensive taxonomy of computer crime that identifies how computer crimes may be classified, based upon the dual characteristics of the role of the computer and the contextual nature of the crime. The thesis also proposes a universal classification code for categorizing computer crime, based upon the work done by this thesis. Additionally, Chapter 3 reveals the differences and similarities in computer crime and cybercrime
legislation alignment with the CoE Convention on Cybercrime in Australia, the UAE, the UK and the USA. While the USA is fully aligned with Articles 2 to 11 of the Convention, Australia and the UK are largely aligned with the Convention and the UAE is the least in alignment with it.

In Chapter 4, the thesis identifies the differences and similarities between two historically and culturally different police organizations, the QPS in Australia and ADP in the UAE, in terms of how they cope with computer crime. This thesis reveals that there are some important issues that continue to create problems for the law enforcement agencies, such as insufficient resources and coping internationally with different national computer crime legislation. It highlights the importance of having comprehensively-documented procedures and guidelines for combating computer crime.

In Chapters 5 and 6, the thesis presents the most comprehensive study currently available regarding the amount of money laundered concerning four such developed or fast-developing countries. It presents a comprehensive cross-jurisdictional analysis of the figures representing the extent of money laundering in Australia, the UAE, the UK and the USA. The thesis found that there are considerable variations in the estimates of the extent of money laundered in these four countries.

This thesis identifies that the UK and the USA are the most advanced with regard to anti-money laundering and combating the financing of terrorism (AML/CFT) systems among the four countries, based on compliance with the FATF recommendations. Australia and the UAE have further to go to be compliant with the FATF recommendations, and the UAE, in particular, is the least compliant with these recommendations among the four studied countries. The thesis identified that local factors have affected how the UAE has implemented its financial and AML/CFT systems. This research will be of interest to policy makers and law enforcement agencies involved in resolving money laundering and its successful detection and prosecution.

Chapter 7 concludes the thesis with a summary of the research findings and conclusions, and provides a discussion on various areas of possible future works that have been identified.
1.4 Conclusion

This chapter provides an overview of the research presented in this thesis and the research objectives and questions upon which it is focused. The chapter describes the importance of identifying and comparing different approaches for combating computer crime and summarizes the contributions of the research. The nature of computer crime and the existing approaches used for combating such crime are discussed in Chapter 2.
Chapter 2
Computer Crime: Past and Present

Chapter 1 introduced this research and the importance of combating computer-related crime. This chapter reviews the nature of computer crime and how the world tackle such crimes.

The first section (Section 2.1) appraises the different definitions and taxonomies of computer crime that are in use or have been proposed, and the global extent of computer crime.

Section 2.2 examines national approaches and international initiatives to combat computer crime or cybercrime. The section examines the international initiatives represented by the EU, CoE, G8, UN and Interpol in countering computer crime or cybercrime. It also discusses computer crime and cybercrime legislation in Australia, the UAE, the UK and the USA and their government initiatives, and the procedures used by their law enforcement agencies to combat computer crime. These countries have been selected for reasons explained in Chapter 1.

Section 2.3 examines the approaches used by the above-mentioned countries in combating money laundering. Section 2.4 discusses the limitations, challenges and issues surrounding the existing approaches for combating computer crime described in the previous sections and the consequent motivation for the research presented in this thesis. Section 2.5 describes the research methodology adopted in this research in order to answer the research questions presented in Chapter 1. Section 2.6 summarises this chapter.

2.1 Computer Crime

The aim of this section is to provide an overview of computer crime. The first subsection in this section introduces the concept of computer crime and cybercrime
and discusses the different terms that have been used to describe computer-related crime. The second sub-section discusses different taxonomies of computer crime. The last sub-section examines how widespread computer crime or cybercrime is in a global context.

### 2.1.1 Definitions

As indicated in Chapter 1, there are at present a large number of terms used to describe crime involving computers. Such terms include *computer-related crime, computer crime, Internet crime, e-crime, digital crime, high-tech crime, online crime, electronic crime, computer misconduct, and cybercrime.* Historically, cybercrime referred to crimes happening over networks, particularly the Internet, but that term has increasingly become a general synonym for computer crime. The Cambridge Advanced Learner’s Online Dictionary defines cyber as a prefix which means “involving, using or relating to computers, especially the Internet: cybercrime; cyberculture”. From that, the definition of cybercrime is a crime related to computers; and especially the Internet.

Donn Parker was one of the first people who wrote on computer crime, and he was then considered the first national expert on computer security in the United States. He used the term *computer abuse* instead of using the term *computer crime,* “because the word abuse allows him to avoid having to differentiate between what is a crime and what is not”. Parker (1976) defines computer abuse as “any intentional act in which one or more victims suffered or could have suffered a loss, and one or more perpetrators made or could have made profit”.

According to Keyser, the USA Department of Justice defines computer crime as “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution”. This seems unnecessarily broad as including ‘prosecution’ could include (for instance) psychological profiling of a modern day Jack the Ripper, yet serial killings would not appear to most people to be a computer crime. The UK Association of Chief Police Officers (ACPO) has defined e-crime as the “use of networked computers, telephony or Internet technology to commit or facilitate the
2.1 Computer Crime

commission of crime”, consistent with the original, network-specific, origins of the term cybercrime.

In his book ‘Cybercrime: The Transformation of Crime in the Information Age’, Wall [34] notes that the term cybercrime “has a greater meaning if we construct it in terms of transformation of criminal or harmful behaviour by networked technology, rather than simply the behaviour itself” and interprets the term cybercrime broadly to refer to “criminal or harmful activities that involve the acquisition or manipulation of information for gain”.

Symantec Corporation [19] 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 also includes crimes that happen within a stand-alone hardware device or computer. Kshetri [1] analyses cybercrime and its motivation in terms of cost-benefit to the cyber-criminal and defines cybercrime as a crime that utilises a computer network during the committing of the crime such as online fraud, online money laundering, identity theft, and criminal uses of Internet communication. This definition requires the crime to be committed over the computer network to be considered as a cybercrime. Others define cybercrime in terms of different categories based on the type of the committed crime. For instance, the Foreign Affairs and International Trade of Canada [14] defines cybercrime as a crime that is committed using computers and networks (e.g., hacking and computer viruses) and the facilitation of traditional crime 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. The Australian Centre for Police Research (ACPR) [17] defines e-crimes (cybercrime) as “offences where a computer is used as a tool in the commission of an offence, as the target of an offence, or used as a storage device in the commission of an offence”. Wilson [35] has defined cybercrime into two categories: crime that targets computers and crime that is enabled by computers. These definitions, in fact, may in part be the result of categorising computer crime or cybercrime under different groups and
may not necessarily exemplify the real meaning of the term computer crime or cybercrime.

Grabosky [36] suggested 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, in contrast, Wall [37] described cyberspace and the new types of crime as “new wine, no bottles”. However, generally and as indicated previously, the term cybercrime involves not only new crimes against computer data and systems, but also traditional crimes such as fraud. The USA Department of Justice, Computer Crime and Intellectual Property Section [38], indicated that whether cybercrime is classified as “old” crime or “new” crime, it “creates unique problems for law enforcement and a concomitant threat to the public welfare”. Under the CoE Convention on Cybercrime, the term cybercrime refers to offences against confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; and offences related to infringements of copyright and related rights [20]. But, it is still not clear how the CoE definition covers other offences such as identity theft.

Under the Cybercrime Act 2001 of Australia, the term cybercrime refers to crimes that target computer data and systems. Yet, the UAE Federal Law No. (2) of 2006 on The Preventive of Information Technology Crimes provides a very broad meaning for the term computer crime or cybercrime to include all offences against computer data and systems, computer-related offences (e.g., forgery, fraud, money laundering, threats), content-related offences (e.g., child pornography) and other offences such as those that violate religious beliefs or threaten and violate family principles. The USA Department of Justice, Computer Crime and Intellectual Property Section, defines computer crime or cybercrime as any crime that utilises or targets computer networks and refers to viruses, worms, and DoS attacks [18]. Though this definition is clearly covering the crimes that target computer data and systems, it also covers the use of a computer to commit traditional crime. The UK Computer Misuse Act 1990 has similar provisions on crimes against computer data and systems. However, the UK Association of Chief Police Officers (ACPO) [33] 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 Australian Crime Commission (ACC) noted that the expressions computer crime, e-crime, high-tech crime and cybercrime all refer to the same type of crime [17]. Indeed, the ACC cites the definition of e-crime used by the Australian Centre for Police Research (ACPR) to define cybercrime. According to the ACPR, e-crime is defined as “offences where a computer is used as a tool in the commission of an offence, as the target of an offence, or used as a storage device in the commission of an offence” [17].

It is apparent from the above, that the terms computer crime and cybercrime are interpreted differently by different jurisdictions. As a result, not all computer crime around the globe is treated and criminalised in the same way in each country. That is, one computer activity could be a crime in one jurisdiction and not a crime or computer crime in another jurisdiction. This thesis is concerned with both computer crime and cybercrime – that is, both crimes involving stand-alone computers or devices or networks, and crimes undertaken via the Internet. As indicated in Chapter 1, this thesis generally therefore uses the two terms computer crime and cybercrime more or less interchangeably, using the latter term in its broad sense, but distinguishing between criminal activity involving stand-alone systems and criminal activity involving the Internet where necessary. Consequently, for the purposes of this thesis, we define computer crime broadly as any crime that utilizes or targets computer data and systems for committing an illegal activity.

2.1.2 Taxonomies

There are considerable differences regarding what specific crimes are encompassed by the terms computer crime or cybercrime. Brenner [39] classifies computer crime or cybercrime into three categories:

- the use of a computer as a target of criminal activity (e.g., hacking, dissemination of viruses)
- the use of a computer as a tool or instrument used to commit a criminal activity (e.g., online fraud)
• the use of a computer as incidental to the crime (e.g., data storage for a criminal activity).

Likewise, some others concur with this view (Symantec Corporation [19], Gordon and Ford [13], Sukhai [40], Kelly [12], and the Australian Centre for Police Research [17]).

However, still others classify computer crime or cybercrime into only two categories (see Koenig [41], Furnell [11], Wilson [35], Lewis [42], and the Australian High Tech Crime Centre [43]). Similarly, the Foreign Affairs and International Trade of Canada [14] classifies cybercrime into two categories:

• crime that is committed using computers and networks (e.g., hacking and viruses)
• traditional crime that is facilitated through the use of computers (e.g., child pornography and online fraud).

Likewise, the categorisation by Urbas and Choo [44] identifies two main types of computer crime or high-tech crime: 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. Figure 2.1 illustrates the Urbas and Choo computer crime classification.

Figure 2.1 Types of high-tech crime classification (Adapted from [44])
Other classifications have elaborated on the above in one way or another. However, despite some considerable differences, there is a core of consistency between some of the above classifications. It is becoming increasingly accepted that the computer system plays two main roles in cybercrime:

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

We concur with this view and most of the remainder of this chapter is based upon that premise except where otherwise stated.

In contrast to the above computer crime and cybercrime classifications, there are other classifications still, some of which include consideration of factors other than the role a computer system plays in the committing of computer-related crime. These factors include: threats (Thomas [45]), attackers (Kanellis et al [9]), attacks (Kanellis et al [9], Chakrabarti and Manimaran [46]), motives (Kanellis et al [9], Thomas [45] and Krone [47]), and victims (Sukhai [40] and Sabadash [48]). We now discuss some of these other classifications, in particular classifications emerging from the UN, the CoE and the G8. The UN manual on the prevention and control of computer-related crime [49], published in 1999, lists common types of computer crime as in Figure 2.2.

![Figure 2.2 The common types of computer crime according to the UN (Adapted from [49])](image-url)

Though the UN manual includes crimes against computer data and systems, it also covers some crimes that utilise 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. Yet, the Council of Europe (CoE) Convention
on Cybercrime classifies computer crime or cybercrime into four main categories as illustrated in Figure 2.3 [20].

We note that the CoE categorisation does not include some types of crimes that have been committed or facilitated using the computer such as money laundering and identity theft.

At the G8 Government/Industry Conference on High-Tech Crime [50] in 2001, the participants discussed the need to categorise high-tech crime according to the type of threat, not the type of crime. The reason for this was to avoid the problem posed by variations in criminal law across jurisdictions which in turn results in varying local definitions of high-tech or computer crime. This however raises some other (semantic) problems and we discuss this point further below. The conference noted that the CoE classification is not comprehensive and does not address all computer-assisted threats. The conference workshop divided threats into two major categories as follows [50] (also see Figure 2.4):

- Computer infrastructure attack: “operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves”.

Figure 2.3 The CoE taxonomy of cybercrime offences (Adapted from [20])
2.1 Computer Crime

- Computer assisted threat: “malicious activities ... which are facilitated by a computer. The computer is used as a tool in the threat or offence”.

![Diagram of G8 taxonomy of threats]

Figure 2.4 The G8 taxonomy of threats (Adapted from [50])

We can observe from the G8 classification some interesting points. Firstly, the ‘computer infrastructure attack’ category is meant to cover all crimes where the computer or computer network is a target of criminal activities. In fact, this category of threat that covers all types of attacks on computers and computer networks is widely accepted. Secondly, the ‘Computer assisted threat’ category includes threats that are facilitated by computers or computer systems, which we discussed earlier as the utilisation of computer systems to commit a crime.

2.1.3 Global Extent of Computer Crime

Computer crime or cybercrime is the FBI's number three priority [1, 2]. Also, according to the FBI’s estimation, computer crime in the USA costs industry about $400 billion in 2004 [3, 4]. According to Reuters, 2006, the Department of Trade and Industry in the UK says that computer crime has increased by 50% over the last two years (2004 and 2005) [3]. At the International level, high-technology crime is one of Interpol's top five priorities [5].
Statistics on the scale of computer crime or cybercrime are mostly estimations based on surveys. According to the Australian Computer Crime and Security Survey [51], the total average loss per organisation in 2006 for computer crime, electronic attack, and computer misuse or abuse has increased 63% per organisation compared to 2005. Also in USA, according to the IC3 2005 Internet Crime Report [52], the IC3 (Internet Crime Complaint Center) received 231,491 complaints in 2005 which is 11.6% more than 2004 complaints. In Japan, there are 1,802 cybercrime reported cases to the National Police Agency in the first half of 2006 which has increased by 11.8% compared to the first half of 2005 [53].

The UK National Hi-Tech Crime Unit (NHTCU) estimates the cost of cybercrime on companies based in UK is at least US$4.61 billion in 2004 [21]. Also, according to the USA Treasury Department, the proceeds from cybercrime have overtaken the proceeds from illegal drug sales netting an estimated US$105 billion in 2004 [22, 23]. In addition, according to IDC report, a market research firm based in the USA, the 2003 showed more than 60% of computer hackers have targeted financial institutions [1]. Besides that, the total loses in 2006 from Phishing attacks increased to $2.8 billion which is double the total lost in 2004 [54]. Kshetri (2009) indicates that cybercrimes is costing consumers and businesses such as banks and credit card companies billions of American dollars each year [55]. He indicated that the crime rate is linked to the economic opportunities which contribute to motivation for committing a computer crime. The cost of cybercrime is high and without forgetting the cost of controlling cybercrime that is being spent from the organisations which are relying on their computer technology to do business [5]. In conclusion, the cost of computer crime to society is very high and can cause many problems such as facilitating the transfer of proceeds of crime. This thesis therefore also focuses on money laundering which is discussed in more detail under Section 2.3.

### 2.2 Combating Computer Crime

This section reviews national and international approaches for combating computer crime and cybercrime. The first sub-section examines the initiatives of international bodies such as the United Nations (UN), European Union (EU), Council of Europe (CoE), Group of Eight (G8) and Interpol in countering computer
and cybercrime at the international level. Sub-section two provides a very brief summary of relevant legislation in the four countries studied in this thesis and notes that this is then dealt with in detail in Chapter 3. The third sub-section investigates the various government initiatives in Australia, UAE, the UK and the USA to combat computer crime. The last sub-section discusses how police forces in these four countries combat computer crime and cybercrime.

### 2.2.1 International Initiatives to Combat Computer Crime

This section discusses the efforts of international organisations in countering computer crime or cybercrime. The study investigates what the UN, EU, CoE, G8 and Interpol do regarding preventing and countering computer crime and cybercrime.

**United Nations (UN)**

The UN is an international and worldwide organisation. Its goals are to facilitate and support the collaboration in international law and security, economic development, social progress and in solving human rights issues [56]. The UN has many agencies that are working to implement the organisations’ main principles. In fact, one of the UN agencies is the United Nations Office on Drugs and Crime (UNODC) which is responsible for assisting members in combating crime [57]. In 2000, the *UN Convention against Transnational Organised Crime* was adopted in order to fight transnational organised crime [58]. It intends to facilitate a legal framework for international cooperation in countering criminal activities and the increasing connections between terrorist crimes and transnational organised crime [58]. In 2001, the UN produced a report called ‘Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime’ [59]. The report recommends setting strategies and enhancing international cooperation to counter and prevent computer crime [59].

Furthermore, during the Eleventh United Nations Congress on the Prevention of Crime in 2005, there was a workshop on measures to combat computer-related crime [60]. There was a discussion as to what should be done about collaboration between countries and private sectors in combating computer crime. The
workshop concluded by giving the following recommendations in order to combat computer or cybercrime [60]:

- The UN should assist member countries in combating computer crime
- UNODC should provide the technical support and training to the member countries
- Enhancing and encouraging international law enforcement collaboration
- Encouraging the member states to update their legislation and strength their computer crime laws
- Collaborating work between governments, non-governmental organisations and the private sector should take place to counter computer crime.

The International Telecommunication Union (ITU) was established by the UN as a specialised agency for telecommunications [61]. It coordinates the global use of telecommunications and improves the telecommunications infrastructure in the developing world [61]. The ITU also addresses current global challenges such as strengthening cyber security. Following the UN General Resolutions on “Combating criminal misuse of information technology”, the ITU took the lead for “Building confidence and security in the use of information and communication technologies” [62]. In 2009, ITU developed the ‘ITU Toolkit for Cybercrime Legislation’ which is designed to “provide countries with sample legislative language and reference materials that can assist in the establishment of harmonized cybercrime laws and procedural rules” [62].

In April 2010, the UN members rejected a proposal for a global cybercrime treaty [63]. There were many reasons behind this rejection which includes not reaching agreement on some issues such as transferring of digital evidence, and that such a treaty would take a long time to resolve, and the EU and USA view that there is no need for a new treaty since the CoE Convention exists [63].

**European Union (EU)**

The EU consists of 27 European countries [64]. The EU’s member countries are working together through the EU in combating cybercrime and cyber terrorism. The EU enhances cross-border cooperation between member countries. Indeed,
the EU’s Commission and the Council of the EU are focusing a lot of effort on combating cybercrime. In January 2001, the EU’s Commission adopted a statement on “Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime” [65]. The statement emphasised that an inclusive policy program to counter cybercrime should include at least the following four key conditions [65]:

(1) The adoption of adequate, substantive, and procedural legislative provisions to deal with both domestic and transnational criminal activities; (2) The availability of a sufficient number of well-trained and well-equipped law enforcement personnel; (3) The improvement of the cooperation between all stakeholders, users and consumers, industry, and law enforcement; and (4) The need for ongoing industry and community-led initiatives.

Researchers from the EU have collaborated and worked together with academics and people from the IT industry to develop standards for the investigation of computer or cybercrime. The main achievement in combating computer crime from the collaborative work that has been done was the development of the EU Cyber Tools On-Line Search for Evidence (CTOSE) [66]. The CTOSE project is a research project funded and supported by the EU’s Commission. The CTOSE project has developed a methodology that “identifies, secures, integrates and presents electronic evidence” [66].

**Council of Europe (CoE)**

The CoE [67] was established in 1949 and has now 47 member countries. In addition, there are five countries that are attending the CoE’s meetings as observers which include the USA and Canada [67]. The CoE addressed the rising threats created by computer-related crime from the late 1980s [68]. After that, in 1989, the CoE published a study and suggestions which indicated the need for laws criminalising unlawful acts using computer networks. From that time on, the CoE was involved in many projects in combating computer crime or cybercrime. Indeed, in 2001, 29 CoE’s member countries and the USA signed the Council of
Europe Convention on Cybercrime [68]. The Cybercrime Convention requires from the members the following [69]:

- Develop laws against cybercrime
- Make sure that the law enforcements have the essential procedural authorities to investigate and prosecute cybercrime offences
- Supply global collaboration to other countries to combat cybercrime.

Articles 2 to 10 of the CoE Convention describe the types of cybercrime offences and Articles 11 to 22 indicate that the member countries should adopt legislation that establishes ancillary liability and sanctions, procedural law, and jurisdiction. Articles 23 to 35 refer to international cooperation and mutual assistance. Articles 36 to 48 describe signature, entry into force, accessing, effects and others for the purpose of this Convention.

Currently, on the 19th of May 2010, the CoE Convention on Cybercrime has 47 member countries of the CoE and nine non-member countries [70]. The CoE Convention on Cybercrime opens first for signature before it enters into force² for the CoE member countries and also for non-member countries. The CoE Treaty Office (2010) indicated that 46 member countries of the CoE and non-member countries had signed the CoE Convention on Cybercrime, although only 17 of them had entered it into force [70].

**Group of Eight (G8)**

The G8 is a group of eight of the world's main industrial countries. The G8 countries are Canada, France, Germany, Russia, Italy, Japan, the UK and the USA [71]. The G8 focused on combating crime such as its work on transnational organised crime. The G8 established five Subgroups of the Lyon Group to employ and adopt the forty recommendations developed by G8. One of the G8’s subgroups was the G8’s Subgroup on High-Tech Crime. The G8’s Subgroup on High-Tech Crime assists, advises and helps the member countries in combating cybercrime. It offers some recommendations to help its members review their legislation to

---

² According to the third paragraph of Article 36 of the CoE Convention on Cybercrime:

*In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.*
ensure that high-tech illegal acts are criminalised by all member countries [72]. In conclusion, G8 encourages its members to enhance their own laws in particular areas of concern to the G8 such as organised crime, high-tech crime, and terrorist communications and organisations.

**Interpol**

The International Criminal Police Organisation, widely known as Interpol, is an organisation that facilitates the collaboration between all of the police forces around the world. The organisation consists of 186 member countries [73]. Interpol developed and implemented an international police communications system called 1-24/7 [73]. The purpose of this system is to enable and facilitate the exchange of information among the member police forces. The police forces from the member countries can look for and verify data with direct access to Interpol’s databases [73]. In fact, Interpol supports and facilitates the international collaboration among the police forces in combating worldwide crime such as cybercrime. Cybercrime is considered by Interpol as one with the greatest increase in scale and quantity among other crimes [74]. Because Interpol has facilitated a secure communications system for collecting, storing, analysing, sharing and requesting information, the member countries can retrieve data from the system's database with regard to criminal activities such as cybercrime [73]. The system supports the members 24 hours a day, 7 days a week [74]. Moreover, other features of Interpol’s work on combating cybercrime are designed to [74]:

- Assist cooperation between the member countries via a list of contact officers reachable for cybercrime investigation
- Enhance the exchange of information on cybercrime between the member countries
- Support member countries in the incidence of cybercrime investigations or attacks
- Build up partnerships with other international and private organisations.

Also, Interpol has established collaborative work with the private sector in countering the spread of computer crime or cybercrime. For example, Interpol and Microsoft organised the meeting of the BotNet Task Force (initiated by Microsoft
in 2004) to tackle and address the growing threats of Botnets [75]. Additionally, Interpol and the G8 High Tech Crime Group support the recommendations provided by the USA and the UK law enforcement agencies for changes to the Internet Corporation for Assigned Names and Numbers (ICANN) [76]. The USA’s FBI and the UK’s Serious Organised Crime Agency (SOCA) proposed that the ICANN should conduct customer due diligence and impose stronger rules on registers for generic top-level domains (gTLDs) such as ‘.com’ [76]. They aim to make it very difficult for criminals to register domain names under fake or false identifications.

2.2.2 Computer Crime and Cybercrime Legislation

Computer crime or cybercrime are increasingly becoming major threats to national and international governments in the digital era. In recent years, jurisdictions worldwide have been forced to evaluate their legal systems to deal with the growing threats of computer-related crimes. For that, the aim of this subsection is to investigate and identify current computer crime and cybercrime legislation in Australia, the UAE, the UK and the USA. The thesis also discusses briefly state legislation in the state of Queensland in Australia. It is noted that Abu Dhabi employs only the federal legislation to combat computer crime. State legislation in the other states of Australia, in the UAE and in the USA is outside the scope of the thesis. Extra detail in relation to the computer crime legislation in the four countries is discussed in Chapter 3.

Australia

The Commonwealth of Australia is a federation of six states and two territories [77]. The Australian constitution (section 51) allocates to the Commonwealth of Australia at the national level certain topics; one of which is post and telecommunications. Another is the external affairs topic which results in the Federal Government having exclusive jurisdiction to negotiate agreements with other national jurisdictions. Remaining topics that are not detailed in section 51 remain with the States. The main instrument in Australia for combating computer crime or cybercrime is the Cybercrime Act of 2001. Cybercrime can only be affected via a telecommunications service and as such the Cybrecrime Act 2001 is
the principal enactment covering computer crime or cybercrime in Australia. In fact, the Cybercrime Act 2001 is influenced by the Computer Misuse Act 1990 of the UK\textsuperscript{3} [78]. The Cybercrime Act amends a number of statutes, including the Criminal Code Act 1995 (Cth) [79]. The Act inserted Part 10.7, Div 467, Div 477 and Div 478, into the Criminal Code to cover computer-related offences.

In 1989, the Federal Government amended its Crimes Act with provisions to deal with computer crime [80, 81]. Indeed, this amendment was the first article of legislation by the Federal Government regarding computer crime. In 1991, the Telecommunications Act of 1991 added sections 74 and 76 to the Australian Criminal Code [82]. Section 74 defines ‘carrier’ and ‘data’, and section 76 discusses the criminalisation of unauthorised access to Commonwealth computer systems. It also criminalises the examination, alteration, modification and damaging of data [82]. In 1995, the Criminal Code Act was amended to address new computer crimes such as hacking and spreading of viruses [81].

Subsequently, additional advances in technology and the Internet have led the Australian Government to update its legislation to cover new computer crime. In 2001, the Government introduced the Cybercrime Act 2001 [81]. The Act came into effect in Australia in 2002 [81]. The Act amends the law relating to computer offences and introduces the following offences to the Criminal Code Act 1995 [79, 81]:

**Division 477**: consists of the following sections:

- *Section 477.1*: Unauthorised access, modification or impairment with intent to commit a serious offence
- *Section 477.2*: Unauthorised modification of data to cause impairment
- *Section 477.3*: Unauthorised impairment of electronic communication.

**Division 478**: the offences under this division are:

- *Section 478.1*: Unauthorised access to, or modification of, restricted data
- *Section 478.2*: Unauthorised impairment of data held on a computer disk etc.
- *Section 478.3*: Possession or control of data with intent to commit a computer offence

\textsuperscript{3} See Cybercrime Bill 2001 Digest No. 48.
• **Section 478.4**: Producing, supplying or obtaining data with intent to commit a computer offence.

Additionally, all of the Australian States and Territories have also provisions for criminalising computer crime [80]. For instance, the Criminal Code Act 1899 of Queensland has provisions on computer-related offences under the following sections [83]:

- **s 359E**: Punishment for unlawful stalking
- **s 398**: Punishment of stealing
- **s 408C**: Fraud
- **s 408D**: Obtaining or dealing with identification information
- **s 408E**: Computer hacking and misuse.

**UAE**

The United Arab Emirates (UAE) is a federal country consisting of seven states, also known as emirates [84]. The legal system in the UAE is based on the dual system of Islamic (sharia) and civil law. Until now, the UAE has not accepted the compulsory jurisdiction of the ICJ. Just recently, in 2006, the UAE enacted its first legislation for combating cybercrime. The UAE Federal Law No (2) of 2006 on The Prevention of Information Technology Crimes contains 29 articles that determine cybercrime offences [16]. This law is considered the main legislation in the UAE for making illegal the unlawful use of a computer and computer system. The UAE Federal Law No (2) consists of 29 articles that address cybercrime. Article 1 initially defines terms used in the Federal Law, and the rest of the articles discuss the offences and penalties of committing computer related crimes [85]. Article 2 criminalises the illegal access or access to a site or computer system without authorisation. Article 3 relates to the act of illegal access described in Article 2 in which the acts happen by an inside person when they are doing their jobs or because of this job or facilitate the unauthorised access because of their job. Additionally, money laundering is criminalised under Article 18 of the UAE Federal Law on The Prevention of Information Technology.

The UAE Federal Law No 2 of 2006 covers a wide range of computer or high-tech related crimes. The law was introduced to address the increasing number of
computer crimes occurring in the UAE, and to protect and regulate the lawful
access and use of high-tech services and systems. In conclusion, it is the first step
taken by the UAE government to criminalise computer crime or cybercrime, and
certainly further action is required in order to combat such crimes. Chapter 3
discussed that in more detail.

**UK**

The United Kingdom (UK) has signed the CoE Convention on Cybercrime but has
not ratified it [86]. The legal system in the UK is based on “common law tradition
with early Roman and modern continental influences” and it accepts as
compulsory the jurisdiction of the ICJ, but with reservations [87]. With regard to
computer-related crimes, the UK was one of the first countries to have a computer
crime unit, which was established in 1985 [82]. Then, in 1990, the UK introduced
the Computer Misuse Act 1990 that defines the laws, procedures and penalties
surrounding unauthorised access to computer systems [82]. The Computer Misuse
Act 1990 is the only legislation in the UK that focuses specifically on computer-
related crime.

In 1984 [82], the UK introduced an Act regarding the protection of data called
the Data Protection Act of 1984. This Act explains how data is gathered, used,
disclosed, and disposed, and deals with the procurement and use of private data.
In fact, the UK was one of the first countries to have a computer crime unit which
was established in 1985 [82]. Then, in 1990, the UK introduced an Act that defined
the laws, procedures and penalties surrounding unauthorised access to computer
systems [82]. The Act was called the Computer Misuse Act 1990. Three years after
the introduction of this Act, two UK citizens became the first people to be
sentenced for violating the Computer Misuse Act [82]. The Computer Misuse Act
1990 is the only legislation in the UK which focuses specifically on computer-
related crimes. The Act has introduced the following criminal offences [88]:

- Unauthorised access to any program or data kept or maintained in computer
- Unauthorised access to any program or data kept or maintained in computers
  for the purpose of committing or facilitating further offences
- Unauthorised modification of computer contents, data or programs.
In addition, the Act covered the area of jurisdiction. Section 4 and Section 5 of the Act state that UK courts have jurisdiction if either the offender or the targeted computer (victim) were in the UK [88, 89]. In 2006, the UK introduced the Police and Justice Act 2006 [90]. The Police Act amended the Computer Misuse Act for three reasons: to include longer penalties under Section 1; criminalising Denial of Service (DoS) attacks; and criminalising the supply or offer to supply software/tools that could possibly be used to commit a computer crime [90, 91]. However, the last change has created problems for researchers who use some of the dual use tools, for the good purposes of identifying security flows [90, 91]. More recently, the UK government has come with guidelines that address some of the researchers’ concerns. For example, in order to prosecute the owner of a tool, it needs to identify that the tools were intended to be used to perpetrate computer crime [92]. Conversely, the guidelines have not discussed the distribution of such tools; so, it is still possible to prosecute the person who distributes such tools [92].

**USA**

The USA is a federal country with its laws being allocated between the federal and state legislations. The legal system in the USA is a “federal court system based on English Common Law; each state has its own unique legal system”[93]. Until now, the USA has not accepted the compulsory jurisdiction of the ICJ. The main legislation in the USA concerning computer crime is the Computer Fraud and Abuse Act 1986, also known as Section 1030 of Title 18 of the USA Code (18 USC 1030). The Act covers many computer-related offences [18]. In 2006, the USA ratified the CoE Convention on Cybercrime [86]. In 1977, the first proposal for federal computer crime legislation in the USA was the Ribicoff Bill, which prohibits the unauthorised use of computers [94]. Although the bill was not adopted, this bill became the model for legislation concerning computer crime and it increased awareness of computer crime around the world [94].

The main legislation in the USA concerning computer crimes is the Computer Fraud and Abuse Act 1986. The Act covers many offences related to computers [18]. After the September 11th terrorist attacks in 2001, the Computer Fraud and Abuse Act was amended by the USA Patriot Act of 2001 [95]. The amendments are intended to strengthen the USA against terrorist organisations. On the 29th of
September 2006, the USA joined the CoE Convention on Cybercrime, and in 2007, the Convention came into force in the USA [69]. The Computer Fraud and Abuse Act 1986 makes the following acts as offences [18]:

- Obtaining national security information and unauthorised access to computer
- Compromising confidentiality and obtaining information
- Trespassing in a government computer
- Accessing to defraud and obtain anything of value
- Damaging a computer or information
- Trafficking in passwords or information
- Threatening to damage a computer.

**Summary**

In conclusion, Table 2.1 illustrates the main legislation for combating computer crime and cybercrime used in Australia, the UAE, the UK and the USA.

Table 2.1
The main legislation for combating computer crime and cybercrime used in Australia, the UAE, the UK and the USA

<table>
<thead>
<tr>
<th>Country</th>
<th>The main legislation for combating computer crime and cybercrime</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAE</td>
<td>Federal Law No 2 of 2006 on The Prevention of Information Technology Crimes</td>
</tr>
<tr>
<td>UK</td>
<td>Computer Misuse Act 1990</td>
</tr>
<tr>
<td>USA</td>
<td>Computer Fraud and Abuse Act 1986</td>
</tr>
</tbody>
</table>

### 2.2.3 Government Initiatives to Combat Computer Crime

The previous sub-section reviewed the legislation used in Australia, the UAE, the UK and the USA for combating computer-related crime. This sub-section investigates some of the government initiatives in these four countries and their work in preventing and countering computer crime. Governments around the world have established initiatives to counter computer-related crime. This part investigates the governments’ initiatives in Australia, the UAE, the UK and the USA.
**Australia**

In Australia, the Australian High-Tech Crime Centre (AHTCC) was launched on the 2nd of July 2003 as part of the Australian Federal Police (AFP) [96]. The AHTCC’s role is to [17, 96]:

*Provide a national coordinated approach to combating serious, complex and multi-jurisdictional technology enabled crimes, especially those beyond the capability of single jurisdictions; assist in improving the capacity of all jurisdictions to deal with technology enabled crime; support efforts to protect the National Information Infrastructure (NII).*

The Attorney General’s Department notes that some agencies including the AHTCC and Australian Crime Commission (ACC) have established the Australian Computer Emergency Response Team (AusCERT) [17]. AusCERT provides information security advice to the Australian public, the education sector and its members [97]. AusCERT is based at the University of Queensland and partially funded by the Federal government [17, 97]. Indeed, it is a member of the global organisation of the Incident Responses and Security Teams [17], and in that capacity, AusCERT has “access to accurate, timely and reliable information about emerging computer network threats and vulnerabilities on a regional and global basis” [97]. In November 2009, the Australian Government established its Cyber Security Strategy and, in particular, Australia’s new national CERT - *CERT Australia* - under the Attorney-General’s Department [98]. CERT Australia aims to provide individuals, businesses and government with information regarding cyber threats in order to enhance their protection [98, 99]. On the 15th of January, 2010, Australia’s Minister for Defence opened within the Defence Signals Directorate (DSD) a new Cyber Security Operations Centre (CSOC) in Canberra [100]. The CSOC serves all government agencies of Australia and it has two main roles [101]:

- *it provides government with a comprehensive understanding of cyber threats against Australian interests; and*

- *it coordinates operational responses to cyber events of national importance across government and critical infrastructure.*
The CSOC aims to protect Australian interests from cyber attacks and assess cyber threats against these interests [101].

**UAE**

As mentioned previously, the UAE issued its first cybercrime law in 2006 [85]. From that time, the UAE has increased the focus on the growing threats of crimes involving computers. Because it is a member of the Cooperation Council for the States of Arabian Gulf (GCC), UAE hosted a GCC conference in June 2007, to help member countries enact comprehensive cybercrime legislation [102]. UAE has been the first country from the GCC to pass cybercrime legislation [102].

In April 2007, the UAE government established a new task force to combat cybercrime [103]. The task force is created by the UAE’s Telecommunications Regulatory Authority (TRA) and is called the United Arab Emirates Computer Emergency Response Team (aeCERT) [97, 103]. The aeCERT facilitates the detection, prevention and response to cyber incidents on the Internet [97]. In fact, according to the aeCERT’s website, some of the aeCERT goals are [97, 103]:

- Improve cyber safety and assist in the creation of new legislation in the UAE
- Increase security awareness in the UAE
- Build expertise in information security, incident management and computer forensics
- To be a central trusted point of contact for cyber security incident reporting in the UAE
- Create a nationwide center to distribute information about threats, vulnerabilities, and cyber security incidents.

**UK**

In a report prepared by the Parliamentary Office of Science and Technology, there was a list of agencies involved in combating computer crime. Some of these agencies are [104]:

- **Local police forces**: all police forces in the UK have some structure of computer forensic and investigation ability
• **Serious and Organised Crime Agency (SOCA):** the Serious and Organised Crime Act 2005 has merged the National High Tech Crime Unit (NHTCU) into SOCA which has a computer crime unit

• **National Infrastructure Security Coordination Centre (NISCC):** it works to reduce the risk of electronic attacks on significant national infrastructure

• **Child Exploitation and Online Protection Centre (CEOP):** it runs a website to educate and advise young people and their families about the online safety.

Similar to the Australian version of CERT – AusCERT – the UKCERT provides practical information which is available to anyone who has a responsibility for information security [105]. In fact, it gives advices on current IT security issues [105]. With regard to industry organisations, the Internet Watch Foundation (IWF) is a self-governing organisation which works with the government, police and ISPs to reduce the amount of illegal material on the Internet [104]. The IWF runs a reporting system to assist police forces and ISPs investigate child pornography hosted worldwide [104]. Additionally, the UK established the Cyber Security Operations Centre (CSOC) and it is due to open in 2010 [106]. The COSC aims to monitor and detect threats to UK infrastructure and also it aims to counter such threats when required [106].

**USA**

The Computer Crime and Intellectual Property Section (CCIPS) at the USA Department of Justice has mentioned in its website the primary federal law enforcement agencies that investigate domestic crime on the Internet. These agencies include [107]:

• **The Federal Bureau of Investigation (FBI):** the FBI local office in each state receives reports about the following cybercrime: computer intrusion (e.g. hacking), password trafficking, child pornography or exploitation, Internet fraud and SPAM, Internet harassment, Internet bomb threats, trafficking in explosive or incendiary devices or firearms over the Internet and intellectual property crime
- **The USA Secret Services**: the USa Secret Service investigates the following types of cybercrime: computer intrusion (e.g., hacking), password trafficking, counterfeiting currency, and the Internet fraud and SPAM

- **The USA Immigration and Customs Enforcement (ICE)**: the ICE receives reports about the child pornography or exploitation if they are imported to the USA and intellectual property crime

- **The USA Postal Inspection Service**: the agency receives reports and investigates cases about the child Exploitation and Internet fraud matters that have a mail nexus

- **The Bureau of Alcohol, Tobacco and Firearms (ATF)**: the agency investigates computer crime that is related to its work.

  Additionally, the Internet Crime Complaint Center (IC3) [107] is a centre for receiving, developing and referring criminal complaints about computer crime or cybercrime to the related authority at the federal, state and local level. The agency is a partnership between the FBI and the National White Collar Crime Center (NW3C) [107]. IC3 serves as a central reporting mechanism for complaints involving Internet related crimes [107].

  The CCIPS website describes other government initiatives to combat computer crime. These government initiatives include the STOP initiative and the National Intellectual Property Rights Coordination Center [107]. The STOP initiative provides information to customers and businesses on intellectual property and advises how to report trade in fake goods. One of the National Intellectual Property Rights Coordination Center responsibilities is to coordinate the USA government domestic and international law enforcement activities involving intellectual property rights issues [107].

  In March 2010, a bill was introduced in the USA Senate that will see that “the president [of the USA] would provide an annual assessment on international cybercrime and would be able to suspend aid, financing or trade programs with countries that fail to improve [on combating computer or cybercrime]” [108]. The USA wants to identify computer crime or cybercrime havens. Such criminal activity knows no boundaries and therefore, without international reporting and
cooperation, it would be difficult if not impossible to combat computer-related crime [108].

2.2.4 Law Enforcement Approaches to Combat Computer Crime

This sub-section discusses the approaches and practices for combating computer crime of law enforcement agencies in Australia, the UAE, the UK and the USA. It aims to give an overview with some examples of such approaches, but it is not meant to cover every state or federal law enforcement agency approach. Also, it is important to emphasize here that this sub-section relies mainly upon the available information in the public domain. Overall, this sub-section discusses each country’s approach under the following two headings:

- Policy and procedures
- Technology and staff resources.

Australia

According to the IMF [109], the Australian population in 2008 was around 21.323 million and the Australian GDP was US$ 1,010.70 billion. The Australian culture is described by the Australian Department of Foreign Affairs and Trade [110] as a “diverse culture and lifestyle reflect its liberal democratic traditions and values, geographic closeness to the Asia–Pacific region and the social and cultural influences of the millions of migrants who have settled in Australia since World War II”.

The Australian Federal Police (AFP) and the states and territory police investigate computer crime in Australia. This part examines the efforts of law enforcement agencies in Australia to combat computer crime and cybercrime.

Policy and procedures

The AFP plays an investigative and coordination role within Australia and internationally for multijurisdictional computer crime cases. Generally, for a matter of unauthorised system intrusion, interruption or destruction, in order to be considered to be within the Australian police jurisdiction, one of the following conditions should exist: “the system or computer server where the content is hosted must be in Australia, or the offender causing the intrusion, disruption or
impairment must be an Australian citizen” [111]. With regard to online fraud, the AFP “investigates frauds committed against a Commonwealth Government department or a Commonwealth Authority” [112]. In addition, the policy and procedures category involves two themes: standards and guidelines, and reporting computer crime.

The AHTCC cooperates with relevant law enforcement agencies in Australia and overseas in investigating computer crime [113]. In its website, the AHTCC indicates that it has the following Australian law enforcement partners [114]:

- Australian Federal Police (AFP): the AFP investigates and coordinates within Australia the multi-jurisdictional and international online child sex exploitations cases
- NSW Police: the NSW Police E-crime Unit investigates computer crimes including where a computer is used to attack other computer systems, computer hacking, online auction frauds and sending threatening emails
- Northern Territory Police: the police investigates computer offences where a computer is used to commit a crime or contain an evidence of a crime
- Queensland Police Service (QPS): the Computer Crime Investigation Unit within QPS is responsible for investigating computer crimes such as online fraud and computer hacking
- South Australia Police (SAPOL): the Electronic Crime Section (ECS) within SAPOL investigates computer crimes and provides e-crime prevention programs
- Tasmania Police: the Fraud Investigation Services (FIS) Unit within Tasmania Police investigates computer crimes, frauds and proceeds of crime cases
- Victoria Police: the first Australian computer crime squad was formed by Victoria Police in 1989
- Western Australia Police: the Western Australia Computer Crime Investigation Team performs two main operations: computer crime investigation and computer forensics.

In addition, the policy and procedures category involves two themes: standards and guidelines, and reporting computer crime.
Standards and guidelines

In 2003, participants from different Australian government sectors developed the *Guidelines for the Management of IT Evidence* handbook as part of the Australian Government’s E-Security National Agenda. The handbook addresses many areas such as: definition of electronic evidence, principles for managing electronic evidence, the IT Evidence Management Lifecycle, and the international best practice when dealing with electronic evidence. It intends to present the Australian law viewpoint as to what are the court’s requirements for digital evidence.

Reporting computer crime

Reporting a computer crime depends on the type of the committed crime and the appropriate federal or state investigative agency where the crime should be reported. For instance, the AFP has a team which investigates matters involving children, called the Australian Federal Police Online Child Sex Exploitation Team (OCSET). OCSET carries out the investigation with cooperation within Australia for online child sexual abuse for international and multi-jurisdictional cases. Additionally, the AFP website indicates that the offensive material online and suspicious behaviour online are reported to the Australian Communications and Media Authority (ACMA). Then, ACMA will investigate these matters. Also, AHTCC receives the reports about common computer crimes such as unauthorised access and denial of service attacks. Then, the AHTCC investigates the crime or involves in a collaborative investigation or refers the crime to the related law enforcement or a partner agency [96]. In addition, any crime can be reported to Crime Stoppers Australia. The AFP investigates frauds committed against federal government departments or agencies.

At the state level, the QPS website advises how the victims of online auction fraud should report their complaints. They should first report their complaints to the online auction website and they can give them offenders’ details. Also, determining the offender’s location could be through where the victims send or deposit their money or products. The local police also can assist the victim in finding out the location of the offender. After determining where the offender lives, the complaints are required to be sent to the appropriate law enforcement agency.
Technology and staff resources

We address three aspects of technology and resources: staff resources, computer forensics resources, and education and training.

Staff resources

The number of police officers who investigate computer crime varies from one law enforcement agency to another. For instance, according to the AHTCC website [114], the QPS Major Fraud Investigation Group (MFIG) has “approximately 70 personnel with specialist skills and experience in investigating major and organised fraud-related crimes”. Also, the AHTCC indicates that the Computer Crime Investigation Unit (CCIU) within the MFIG has “five police officers and one administration officer” [114]. Another example of police staffing resources is from Tasmanian Police. Tasmania Police Fraud Investigation Services (FIS) unit that investigates computer crime, frauds and proceeds of crime cases, has “four permanent members and is supported by two on-call forensic computer examiners” [114].

Computer forensics resources

The AFP uses the GetData Software’s forensic investigation tool, Mount Image Pro, to analyse forensic images even if these images are taken by other forensic software such as Encase or Unix DD. Besides that, the Encase software is used by the AFP to analyse digital evidence. In fact, the AFP has a Computer Forensic Section which specialises in acquiring, analysing and presenting digital evidence stored in electronic devices. In March 2008, Microsoft donated the Child Exploitation Tracking System (CETS) tool to the AFP [115]. The CETS tool enables the law enforcement agencies around the world to work together in sharing and tracking information about online child exploitation and abuse [115].

Education and training

The AHTCC joined with Microsoft to provide education and training to Australian law enforcement agencies to combat cybercrime [116]. In 2004, Microsoft trained around 200 law enforcement officials on a wide range of issues related to cybercrime [116]. The focus of the training was on the information sharing procedures, communications protocols, forensic work and tracking down
online paedophiles. In 2005, Microsoft provided the Australian law enforcement agencies with technical training to handle and track illegal Phishing scams and botnets [116].

**UAE**

The IMF [109] indicated that the UAE’s population in 2008 was around 4.764 million and the UAE’s GDP was US$ 260.141 billion. With regard to the UAE culture, it is in many ways considerably different from the culture in Australia, the UK and the USA. The UAE’s culture has developed from a strong belief in Islam which governs people’s way of life, behaviour and decisions [117].

This part discusses the following two main categories: policy and procedures, and technology and staff resources.

**Policy and procedures**

Because the UAE has issued the computer crime legislation recently in 2006, there is not much information yet available about the policy and procedures, and technology and staff resources used to combat cybercrime. With regard to the law enforcement agencies in the UAE, there are seven emirates in UAE and each one maintains its own police force [118]. These police forces are Abu Dhabi Police, Dubai Police, Sharjah Police, Ajman Police, Umm Al Qaiwain Police, Ras Al Khaimah Police and Fujairah Police.

**Technology and staff resources**

In March 2010, 15 police officers from ADP have completed a Master of Science in Information Technology specialization in Cyber Security from Zayed University in Abu Dhabi [119].

With regard to computer forensics training, there is not much information found about the courses available for this type of training. For instance, SANS Institute is organising some training courses in UAE in March 2008, including system forensics, investigation and response course [120]. However, as mentioned in Section 3.3.2, the aeCERT aims to provide security awareness, training, and working as a trusted point of contact for computer incidents [97, 103]. Therefore,
the efforts of aeCERT will have some impact in the fight against computer related crimes.

**UK**

The IMF [109] noted that the UK's population in 2008 was around 61.073 million and the UK's GDP was US$ 2,674.09 billion. Additionally, according to the UK's Embassy in the USA [121], there are many different races and cultures that have had an influence on the UK and therefore played an important part in creating its diverse society and culture.

The London Metropolitan Police Service is the UK's largest police force [122]. This part discusses the following two main categories: policy and procedures, and technology and staff resources.

*Policy and procedures*

In their 2007 report, the London Metropolitan Police Service reported that they are establishing a new police e-crime co-ordination unit to organise the police response to e-crime for the advantage of all of the Association of Chief Police Officers (ACPO) forces, industry and the public [123]. One of the advantages of forming a national e-crime unit is the “opportunity to consolidate disparate methodologies and practices across forces in dealing with e-crime into a cohesive national policy providing policy guidance, best practice and Standard Operating Procedures”, as Metropolitan Police Authority mentioned in their report in 2007 [123]. In the UK and Wales, there are 43 local police forces [124].

In February 2009, the Police Central e-Crime Unit (PCeU) was established within the London Metropolitan Police Service [125]. The PCeU is run by the London Metropolitan Police and it coordinates all 43 local police forces’ e-crime divisions [125, 126]. The e-crime unit focuses on improving basic e-crime training and creating a central reporting web site [125, 126].

The investigation process starts when a crime is reported to the police. Then, that police unit collects basic details of the victim and the incident and records the incident. Then, the police assign the crime to the relevant police force according to the rules regarding jurisdiction. After that, the relevant police force will initiate the
investigation and create a crime record in the appropriate police force crime recording system. However, some police forces omit the incident recording step.

In their website, the UK Metropolitan Police Service has advised how to report a computer crime [127]. The police stated where to report a computer crime according to which of the following categories listed below the crime related [127]:

- **Illegal or offensive material or content on websites, newsgroups etc.:** contact the Internet Watch Foundation (IWF)
- **Hacking and other computer crime:** the crime should be reported firstly to the local police station
- **Offensive e-mails:** police only assist in criminal situations; unless the reporter feels some danger as a result of threatening emails, then contact the local police station
- **Viruses:** police ask to not notify them about viruses, unless the reporter believes the virus is part of hacking or misuse, and then they should contact the police.

Furthermore, the policy and procedures category discusses two themes: standards and guidelines, and reporting computer crime.

**Standards and guidelines**

The UK Association of Chief Police Officers (ACPO) had set guidelines to deal with computer evidence called the “Good Practice Guide for Computer-Based Electronic Evidence” [128]. In 2004, ACPO refined and introduced the fourth version of the guide. The guideline intends to assist the following in [128]:

- Personnel attending crime scenes or making initial contact with a victim/witness/suspect
- Investigators
- Evidence recovery staff
- External consulting witnesses.

To conclude, the guide was produced to address the use of computer evidence during the cybercrime investigation. This guide and similar other guides are
intended to help the investigation officers when dealing with a rapid change and growth area like cybercrime.

**Reporting computer crime**

The victims of computer crime in the UK can report an incident to the police through the following channels [129, 130]:

- Visiting a police station in person
- Make a phone call to the force control room
- Report the incident online via Crimestoppers website.

With regard to recording computer crime in the police database, there are two stages when recording a crime reported to the police. First stage involves recording the incident and collecting basic details of the victim and the incident, and then is assigned to the relevant police force according to the geographical location of the victim for initial investigation. Second stage is when a crime record is created on the related force crime recording system and assigned a local force code to record the offence type [130].

**Technology and staff resources**

We address three aspects of technology and resources: staff resources, computer forensics resources and education and training.

**Staff resources**

In 2007, the E-Crime Section, within the Serious and Organised Crime Authority, had 80 staffing resources [131]. The manpower represents an important aspect in countering computer crime. For that, in 2003, the Guidance Software Company has trained more than 550 UK investigators [122]. While in 2007 the London Metropolitan Police indicated that the PCeU will need eventual staffing requirements of 45 employees [123], it has, in 2009, only 30 employees [132].

**Computer forensics resources**

From January 2003, the London Metropolitan Police Service has selected the EnCase Forensic Edition as its standard tool to combat and investigate computer crime [122]. The selected tool has been used by the police in investigating many
such cases as those involving pornography, virus writing and denial of service attacks. Besides the EnCase tool, London police use a number of FastBloc write-blocking hardware devices to ensure the reliability of the digital evidence [122]. Regarding the type of tools, the Computer Network Defence Ltd organisation provides a list of forensic and anti-forensic tools for the purpose of educating and assisting the computer forensic investigators in understanding the challenges that they may face [133].

Education and training

The staff of police forces receive training courses to raise their awareness and knowledge about computer crimes. Indeed, a number of specialist units within UK police service provide computer crime training for the police forces staff. The UK government has worked with the industry sector to increase public awareness about computer crimes [104]. For instance, 'Get Safe Online' is a joint Government-industry initiated partnership intended to increase computer security awareness among the public and business organisations and educate and advise them in how protect their computer systems from misuse [104, 130]. In 2003, the Guidance Software Company has noted that “more than 550 UK investigators have attended Guidance Software’s forensics courses” [122].

**USA**

According to the IMF [109], the USA's population in 2008 was around 304.415 million and the USA’s GDP was US$ 14,264.60 billion. The USA’s culture has been influenced by different tribes and races and it reflects a combination of multi-cultural groups [134].

This part discusses the approaches and guidelines used in the USA for combating computer crime or cybercrime and dealing with digital evidence developed and applied by particular government agencies. These agencies are: Federal Bureau of Investigation (FBI), Computer Crime and Intellectual Property Section (CCIPS) at the Department of Justice, National Institute of Justice (NIJ), Secret Service and the National Institute of Standards and Technology (NIST).
Policy and procedures

The FBI has a set of approved Standards of Operating Procedures and Quality Assurance Manuals that administrate the policies and procedures concerning the following processes [135]:

- Data gathering
- Evidence handling
- Search and seizure operations
- Examination of seized electronic equipment
- Courtroom testimony.

The “How the FBI Investigates Computer Crime” document intends to give information about some of the guidelines, policies, and resources the FBI uses to investigate computer crime [136]. The document explained the most frequently used legislation by the FBI to investigate computer crimes. The FBI investigates computer incidents if the following conditions exist [136]:

- The incident is a violation of the federal law and within the jurisdiction of the FBI
- The USA Attorney’s Office supports the investigation and the prosecution.
- Also, the information will be gathered in the following ways [136]:
  - Voluntary disclosure of information upon request
  - Court order
  - Federal magistrate judges subpoena
  - Search warrant.

In addition, the policy and procedures category involves two themes: standards and guidelines, and reporting computer crime.

Standards and guidelines

The NIJ is the research development and evaluation agency of the USA Department of Justice. The NIJ has developed and produced a series of guides to address the investigation process. Some of these guides include:
• *Electronic Crime Scene Investigation: A Guide for First Responders (2001)*: this document explains the nature of the digital evidence and the procedures for collection and protection associated with this kind of evidence [137]

• *Forensic Examination of Digital Evidence: A Guide for Law Enforcement (2004)*: this guide aims to explain digital evidence processed [138]

• *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors (2007)*: this guide aims to tell crime scene investigators regarding the legal requirements when dealing with digital evidence [139].

Besides the above guidelines, the NIJ has developed and published other guidelines and tests for forensic tools and write blocker’s hardware and software. Besides that, the CCIPS has also published some guides to assist in investigating and prosecuting computer crimes. Some of these guides include:


• *Prosecuting Computer Crime (2006)*: this guide looks at the federal laws that are related to computer crimes. Such laws include the Computer Fraud and Abuse Act, Wiretap Act, and other network crime statues [18].

With regard to developing standards and measurements for computer forensic tools, the National Institute of Standards and Technology (NIST) is a federal technology agency which aims to develop and promote measurement, standards, and technology [142]. NIST has a project called Computer Forensics Tool Testing (CFTT). The project provides evaluation and verification that the tools used in investigating computer crimes are producing valid results [142].

**Reporting computer crime**

The CCIPS website [107] states where to report computer or intellectual property crime when it is related to the jurisdiction of the federal agencies. Table 2.2 illustrates where to report some examples of computer crime according to its type.
Table 2.2
Type of computer crime and the appropriate federal investigative agencies where the crime should be reported (From [107])

<table>
<thead>
<tr>
<th>Type of Crime</th>
<th>Appropriate federal investigative agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer intrusion (e.g. hacking)</td>
<td>FBI local office&lt;br&gt;USA Secret Service&lt;br&gt;Internet Crime Complaint Center (IC3)</td>
</tr>
<tr>
<td>Password trafficking</td>
<td>FBI local office&lt;br&gt;USA Secret Service&lt;br&gt;Internet Crime Complaint Center (IC3)</td>
</tr>
<tr>
<td>Counterfeiting currency</td>
<td>USA Secret Service</td>
</tr>
<tr>
<td>Child pornography or exploitation</td>
<td>FBI local office&lt;br&gt;If imported, USA Immigration and Customs enforcement&lt;br&gt;Internet Crime Complaint Center (IC3)</td>
</tr>
<tr>
<td>Internet harassment</td>
<td>FBI local office</td>
</tr>
</tbody>
</table>

In addition, the Internet Crime Complaint Center (IC3) is a centre for receiving, developing and referring criminal complaints about cybercrime to the related authority at the federal, state and local level. IC3 serves as a central reporting mechanism for complaints involving Internet related crimes [107]. Also, there are other agencies where the crimes could be reported to, and that all depends on the type of crime. For example, computer crimes that are related to the national security should be reported to the Department of Homeland Security’s National Infrastructure Coordinating Centre.

**Technology and resources**

We address three aspects of technology and resources: staff resources, computer forensics resources and education and training.

**Staff resources**

The BBC news reported in 2001 [143] that the FBI has a squad of more than 200 agents working in computer crime investigation across the USA. In 2008, the USA Department of Justice requested $258.5 million in funding for 659 cybercrime field agents [144]. Indeed, the FBI’s cybercrime field agents represent around 5.5% of the 11,868 agents, the total number of the FBI agents [144].
Computer forensics resources

In 2006, the Guidance Software Company noted [145] that the FBI, the USA Department of Homeland Security, and the USA Department of Defense use the Encase Forensic tool to investigate digital evidence. Also, the FBI and other state and federal law enforcement agencies in the USA also use the Mount Image Pro v2 forensic software [146]. Besides that, the FBI uses the Solitaire Forensics Kit which is a portable hard disk duplication kit used for duplicating and imaging media/hard drives [147]. Lastly, there are 14 Regional Computer Forensic Laboratories in the USA which are coordinated by the FBI to provide forensic analysis to federal and local law enforcement agencies nationwide [148].

Education and training

The CCIPS attorneys provide training to the federal and state law enforcement agencies and other national and international agencies upon request [149]. The type of training is about giving lectures and workshops concerning computer crime and intellectual property. Also, the FBI has an academy to provide training and operations for which the FBI is responsible. In addition, the Federal Law Enforcement Training Center (FLETC) provides training and shares technology with other law enforcement agencies [149]. The National Cyber-Forensics and Training Alliance (NCFTA) facilitates training, security awareness, and conducts computer forensic analysis for local, state, federal law enforcement, businesses and education institutions [150]. Furthermore, the local law enforcement agencies are providing training to their computer crime and cybercrime investigators. For instance, the Florida Department of Law Enforcement Computer Crime Center has many roles including training and research [151].

2.3 Combating Money Laundering

The Internet provides many opportunities for cyber criminals such as organized crime to launder their illegal gain over computer networks. As a result, money laundering has been transformed in the past decade or less by the Internet, giving rise to the new term cyber-laundering. Some countries such as the UAE criminalise money laundering activities happening over the Internet under their computer crime legislation. Therefore, this thesis is also focused on money laundering. While
it is clear that some money laundering does not constitute computer crime or cybercrime, it is clear that money laundering implemented via the Internet does. This section aims to provide an overview of what comprises money laundering and the approaches used to combat such crime at the national and international level. The first sub-section introduces the concept of money laundering and also describes the money laundering process. Sub-section two discusses the international approaches for combating money laundering. The last sub-section examines the approaches used to combat money laundering in Australia, the UAE, the UK and the USA.

2.3.1 Money Laundering

Definitions

There are a variety of definitions for money laundering. The European Commission Glossary of Justice and Home Affairs [152] defines money laundering as “the conversion or transfer of money, assets and property derived from criminal activities to apparently legitimate status by disguising their origin through a variety of financial maneuvers”. The Committee on Payment and Settlement Systems of the Bank for International Settlements [153] defines money laundering as "the attempt to conceal or disguise the ownership or source of the proceeds of criminal activity and to integrate them into the legitimate financial systems in such a way that they cannot be distinguished from assets acquired by legitimate means". Organised crime groups use the process of money laundering to hide the identity and source of large amounts of money generated by various criminal activity including financial crime, drug trafficking, and weapons smuggling [154]. The aim is to deposit the proceeds of crime with financial institutions (e.g. banks) without getting the attention of anti-money laundering regulators. To counter this, regulatory regimes have established systems which monitor every transaction exceeding a certain limit – this covers the operations of financial institutions and other organisations that hold substantial funds on behalf of third parties such as casinos and realtors. The limit is set by each government to identify significant transaction which may then be subject to further investigation.

Society at large and financial institutions in particular have benefited from the Internet and online financial transactions. The Internet helps banks to reduce
internal costs and derive income from a new type of revenue via different service charges [155]. In 2005, McCullagh and Caelli [155] noted that at that time (2005), there were more than 7 million Australian Internet banking users. The number around the world is correspondingly far greater and ever increasing. This together with the transnational nature of online commerce and finance provides an opportunity for criminals to misuse financial systems and carry out widespread money laundering through the Internet [154].

For the purposes of this thesis, money laundering is the process of disguising the origin and identity of “dirty” money – money or value that has been gained through illegal means.

**The process of money laundering**

There are two reasons why criminals want to launder money: the money is evidence of crime and in order to hide legitimate income to avoid income tax in countries which levy income tax [154]. The money laundering process involves three stages: placement, layering, and integration [156-158].

*Placement* is the initial entry of the dirty money into the financial system. The purpose of this stage is to insert the cash into a legitimate financial institution [159, 160], and it is the most vulnerable stage because of the large sums of money or cash involved [161]. Criminals use techniques such as the use of a front company, check caching, or money orders to avoid detection [159]. The success of the placement stage will lead to the next stage, the layering stage.

The aim of the *Layering* stage is to separate illegally obtained money from its origin. It involves a series of transactions such as transferring the money to other local or offshore banks, using the money as payment, or loaning it to another company [156, 157]. The layering stage makes it difficult to trace the money due to the ease of transferring money several times between different accounts, banks and countries [160, 162]. This stage may also involve the continuous depositing and withdrawing of various amounts of money and then purchase and sale of valuable items that obfuscates the money trail [160]. It is a complex step, and when there are many layers or transactions involved there will be more difficulties in tracing the source of the money [162]. The layering stage is important because
the money launderers are trying to conceal the identity of the money when it first entered the financial systems. Then, the money launderers will move to the last stage, the integration stage.

Integration is the final stage in the money laundering process cycle, and involves returning the money back into the legal economy. As a result, the dirty money will be integrated into the financial system and can be used by the criminal(s) for any purpose [154].

2.3.2 International Approaches for Combating Money Laundering

The previous sub-section has discussed the money laundering definitions and process. This sub-section reviews the international effort on combating money laundering which has been represented mainly by the United Nations Office on Drugs and Crime (UNODC), CoE Convention on Laundering, Egmont Group, Society for Worldwide Interbank Financial Telecommunication (SWIFT), World Bank and the International Monetary Fund (IMF), and most importantly the Financial Action Task Force (FATF).

The UNODC has established a Global Programme against Money Laundering (GPML) to help the UN members to combat money laundering crime [154]. The UN helps the countries against money laundering crime to introduce legislation, develop strategies, monitor and analyse the problems, raise awareness, and work with other international initiatives. Furthermore, the UN strategies can include supporting the members with training workshops, training materials, providing expertise, technical assistance, and research and data [154]. The UNODC, through its GPML, aims to [163]:

- support the member countries to develop policies to combat money laundering and the financing of terrorism
- monitor and analyses associated problems
- increase public awareness concerning money laundering and the financing of terrorism
- operate as a coordinator of initiatives carried out jointly by the UN and other international organisations.
Chapter 2: Computer Crime: Past and Present

In 2000, the *UN Convention against Transnational Organised Crime* was adopted in order to fight transnational organised crime [58]. It intends to facilitate a legal framework for international cooperation in countering criminal activities such as money laundering, corruption, offences against cultural heritage and the increasing connections between terrorist crimes and transnational organised crime [58]. Article 6 of the UN Convention against Transnational Organised Crime is concerned with the criminalisation of the laundering of proceeds of crime. Article 7 is concerned with the establishment of measures to combat money laundering. Additionally, the *UN Convention Against Corruption* (UNCAC) was adopted in 2003 and it has provisions on criminalising money laundering [164]. The UNCAC includes some measures to prevent and combat money laundering and confiscate proceeds of corruption.

The *Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime* was approved in 1990 to address money laundering threats [165]. Then, in 2005, the Council of Europe (CoE) Convention on Laundering was amended and also updated to cover the financing of terrorism. The new amended *CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime and on the financing of terrorism* was opened in 2005 for signature [165]. The convention takes into account the international instruments including the FATF recommendations on combating money laundering and financing of terrorism. The CoE Convention on Laundering has 56 Articles which address many areas and measures for combating money laundering and financing of terrorism such as measures to be taken at a national level, international cooperation, cooperation between FIUs and monitoring mechanism and settlement of disputes [166].

The *Egmont Group* facilitates international cooperation and exchange of information among foreign counterpart FIUs [167]. FIUs receive, store, analyse and disclose information collected from the financial and non-financial institutions reports [167]. Because the money generally moves around the world, international cooperation and exchange of information is very important between FIUs in investigating money laundering
The SWIFT is a messaging system that enables financial organisations to connect, exchange financial information securely and regulate financial transactions from around the world [168]. Basically, SWIFT is only a carrier of messages and it moves messages containing information about the transfer of funds between financial institutions [168]. Because the information of the sender and receiver is recorded in the SWIFT messaging system, the money laundering investigators can use this information to trace the money back to its origin. In 2006, the New York Times reported that the SWIFT data was examined by the USA government’s officials to block certain terrorist activity.

The World Bank and the IMF developed a ‘Reference Guide to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT)’ to assist countries in implementing an effective AML/CFT system in accordance with international standards including standards set by the FATF [169]. The World Bank and the IMF also provide training and technical assistance for AML/CFT authorities [169].

The nature and history of FATF

The Financial Action Task Force (FATF) has set the Anti-money Laundering/Combating Terrorist Financing (AML/CFT) standards as contained in the FATF Forty Recommendations 2003 (updated in 2004) and the FATF Nine Special Recommendations on Terrorist Financing 2001 (updated in 2008). Countries from around the world have reformulated their legislative regimes and approaches to bring them into line with international and FATF standards. The FATF was established in 1989 by the G7 in response to increased concern about money laundering [170, 171]. It is an inter-government body which develops and promotes policies to counter money laundering and the financing of terrorism; and examines and evaluates its members’ approaches for combating money laundering and terrorist financing. There are 35 members of the FATF which include 33 countries and two regional organisations (European Commission and Gulf Co-operation Council (GCC)) [172]. The FATF established 40 recommendations on anti-money laundering (AML) and 9 special recommendations on combating the financing of terrorism (CFT) to establish a framework for countries to use in order to counter money laundering and terrorist
financing [171]. These recommendations provide international standards to promote and evaluate AML/CFT efforts and many nations like Australia, the UAE, and the G8 countries, have reviewed and continue to review their legislation and regulations to meet the FATF standards. According to the United Nations Office on Drugs and Crime (UNODC) [173], the FATF 40+9 Recommendations provide “a comprehensive set of measures for an effective legal and institutional regime against money-laundering and the financing of terrorism”.

The FATF mutual evaluation program (mutual because member countries evaluate each other) is the main instrument that the FATF uses to monitor the implementation of the FATF recommendations by the member countries [174]. This program evaluates the extent of the AML/CFT systems of member countries and the extent to which they are effective [174]. In 2004, the FATF introduced the ‘Anti-Money Laundering/Combating Terrorist Financing (AML/CFT) Methodology 2004’ to guide the assessment of member countries’ compliance with the FATF recommendations [175]. Also, the AML/CFT Methodology 2004 was updated in 2009 [175]. This methodology was accepted by the International Monetary Fund (IMF) and the World Bank in 2004 [176]. Generally, the FATF team consists of experts from different FATF member countries in the following areas of expertise: legal, financial, and law enforcement [176]. Their expertise should cover all aspects of the effort of combating money laundering and financing of terrorism.

FATF reviews member countries’ compliance with the FATF 40+9 recommendations through essential assessment criteria. These criteria represent elements of each of the recommendations that demonstrate if the member country is compliant. In fact, for each of the FATF 40 recommendations and the FATF 9 special recommendations, there are four levels of compliance:

- **Compliant** – the member country is fully compliant with the recommendation
- **Largely compliant** – the country complies with the majority of the essential criteria

---

4 Also, according to the FATF, in some circumstances, a recommendation may be rated not applicable if a “requirement or part of a requirement does not apply, due to the structural, legal or institutional features of a country e.g. a particular type of financial institution does not exist in that country”. In fact, this is not the case with regard to the four countries under this study.
• *Partially compliant* – the member country complies with some of the essential criteria

• *Non-compliant* – the country does not comply with the majority of the essential criteria.

Once the FATF assessment evaluation team has completed the review of a country's AML/CFT system, it produces a mutual evaluation report which summarises the AML/CFT measures in place and identifies any deficiencies that exist. According to the FATF [177], “[t]here are three types of process that could occur following the discussion and adoption of a mutual evaluation report”:

• Firstly, within two years, the assessed country must report to the FATF with the new measures that have been updated to deal with identified deficient areas.

• Secondly, an assessed country will go through a regular follow-up process when there are major deficiencies in its AML/CFT system especially where any of the core recommendations 1, 5, 10, 13, SR II, and SR IV or the key recommendations 3, 4, 23, 26, 35, 36, 40, SR I, SR III and SR V [178] are rated either partially compliant or non-compliant. Table 6.2 in Chapter 6 illustrates the principles of each one of the core and key recommendations in more detail. Additionally, any country which is subject to the follow-up process has to report back to the FATF Plenary with an update concerning its new measures and improvements in addressing the areas where there are deficiencies.

• Thirdly, a country not complying with the FATF recommendations will go through an enhanced follow-up policy that could result in suspending the country’s membership of the FATF until it implements the recommendations.5

The removal from the regular follow-up process will be based on the procedures that are agreed on by the FATF Plenary in October 2008 [177]. These procedures indicate that the core and key recommendations should be implemented in a country’s AML/CFT system at a level equivalent to compliance or equivalent to largely compliant.

5See the Third Round of AML/CFT Evaluations Processes and Procedures document, paragraph 42.
2.3.3 National Approaches for Combating Money Laundering

The sub-section reviews legislation enacted in Australia, UAE, the UK and the USA to combat money laundering. It also discusses the process of investigating money laundering and the reporting requirements in these four countries. A complete discussion concerning these four countries approach is discussed in Chapter 6.

Anti-money laundering legislation

This part discusses the number and types of offences that are considered to be money laundering under existing legislation in Australia, UAE, the UK and the USA.

Though money laundering is an offence which is criminalised in all four countries – Australia, the UAE, the UK and the USA – there are some significant differences with regard to the nature and number of offences that are considered to be money laundering. According to the Australian Institute of Criminology [179], there are 19 different offences of money laundering in Australia under Division 400 of the Criminal Code Act 1995 (Cth). These offences can be classified into two types: offences related to the proceeds of crime and offences related to the instruments of crime. The same source indicates that “Australia is alone in differentiating between offences based on the value of the funds involved and the degree of knowledge of the offender”.

In contrast to Australia’s 19 offences of money laundering, the USA, UK and the UAE each have three separate core offences that focus on the proceeds of crime [179]. In terms of the USA, the Australian Institute of Criminology [179] observed the following three core offences of money laundering:

(a) conducting a transaction using the proceeds of crime with the intent to disguise its origins, avoid a transaction report or commit another offence; (b) transporting the proceeds of crime into, out of, or through the United States with the intent to disguise its origins; and (c) conducting transactions with funds represented as the proceeds of crime.

In the UK, money laundering is defined by the Proceeds of Crime Act 2002 in terms of three main offences and this differs from both Australia and the USA [179]. These three main offences are described by the Australian Institute of Criminology [179] in the following terms:
(a) concealing, disguising, converting, or transferring criminal property or removing it from the United Kingdom; (b) entering into or becoming involved in an arrangement known, or suspected, to facilitate the acquisition, retention, use or control of criminal property by another person; and (c) acquiring, using or possessing criminal property.

In terms of the UAE, money laundering is criminalised under Federal Law No. 4 of 2002. Under Article No. 2 of the law, the following three main offences are considered to be money laundering [180]:

(a) conversion, transfer or deposit of Proceeds, with intent to conceal or disguise the illicit origin of such Proceeds (b) concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of Proceeds (c) acquisition, possession or use of such Proceeds.

It appears that the UAE’s three money laundering offences are similar to the UK’s, but differ from those of Australia and the USA. The main difference between Australia, the UAE, UK and the USA is in terms of the number and the nature of offences of money laundering. Australia has more offences in relation to money laundering and it determines these offences by the amount of funds involved and the intent and knowledge of the offender. In conclusion, the findings suggest that apart from Australia which has 19 different offences for money laundering, the UAE, UK and the USA each only have three separate offences of money laundering.

**Detecting and investigating money laundering**

Many jurisdictions require financial institutions (e.g., banks) and certain non-financial institutions (e.g., insurance companies) to provide several types of reports such as large cash transaction reports and suspicious activity reports. These reports are collected by the FIU in each country which is responsible for investigating money laundering. The FIUs in Australia, the UAE, the UK and the USA are:

- The Australian Transaction Reports Analysis Centre (AUSTRAC) – (Australia)
- The Anti-Money Laundering and Suspicious Cases Unit (AMLSCU) – (UAE)
- The Serious Organised Crime Agency (SOCA) – (UK)
• The Financial Enforcement Network (FinCEN) – (USA).

The reporting of suspicious transactions is considered an essential element in combating money laundering [181, 182]. The information collected from suspicious transactions reports helps law enforcement agencies in money laundering investigations. Also, it is important to mention that having a suspicious transaction reporting system is a fundamental component of the FATF AML requirements [182, 183]. The data from the reports received is deposited into a database and an investigator can access the data to investigate the flow of cash between accounts. The process of investigation of money laundering consists largely of analysing the database containing the received reports from financial and non-financial institutions.

The amount of data generated from reporting suspicious transactions and other reports is huge; therefore, investigators use automated tools such as data mining and transaction correlation tools for data analysis. The important work here occurs in identifying related transactions and correlations between different transaction sets, accounts, names, addresses and other similar information. The individual may have different accounts in different banks possibly under different names. Making such links between transactions on all related accounts held by the same or related individuals is important. Investigators then attempt to trace the assets and conduct further investigations to identify the origin of the money [158]. For instance, AUS TRAC receives more than 10 million financial transaction reports including suspicious transaction reports, each year [183]. These collected reports are very useful for AUS TRAC and other government agencies such as the Australian Taxation Office (ATO) in investigating and detecting money laundering and other criminal activities. McMillen and Woolley [184] noted that according to AUS TRAC, the ATO is the heaviest user of AUS TRAC’s database.

The use of data mining techniques helps in the investigation of money laundering. Such techniques can reduce the time and resources, and can discover correlation between data items. According to Hand, Mannila and Smyth (2001) [185], data mining can be defined as the “analysis of (often large) observational data sets to find unsuspected relationships and to summarise the data in novel ways that are both understandable and useful to the data owner”. Another
definition for data mining is “the collection of automated tools and Artificial Intelligence (AI) techniques that facilitate searching of large data sets to discover hidden or buried relationships among the data” [186]. Applying data mining techniques can increase the quality of intelligence information [187]. Watkins et al. [186] mentioned that some data mining techniques such as neural networks and cluster analysis are suited for investigating money laundering activities.

An example of how the data collected by the FIU in each country is used in investigating money laundering activities

AUSTRAC introduced the data mining tools in 2003 [188]. Also, in the same year, the automated monitoring system of AUSTRAC identified AU$1.5 million transferred to overseas accounts as part of a drug syndicate [183]. In fact, AUSTRAC receives reports from the reporting entities in Australia and then it analyses the data using data mining and transaction correlation tools. It uses an automated system to monitor and examine the flows of funds between Australia and other countries. An example of the usefulness of this system is evident in relation to a case involving tax fraud. A large amount of money that was being transferred from a foreign country to Australia was detected. AUSTRAC conducted an investigation to identify and examine the source and destination of the funds. The investigation found that the person who received the funds had already received AU$18 million in the last five years [183]. In addition, after investigating the person, he was found guilty and was evidently trying to avoid paying tax [183]. From this example, it is observed that the effectiveness of any investigation is based on two essential elements: the quality of the data collected and the technical quality of data analysis.

The investigation starts by analysing the database containing the received reports from financial and non-financial (e.g., lawyers) institutions. Because the number of transactions is large, the investigators use automated tools such as data mining and transaction correlation tools for data analysis. The important work here occurs in identifying related transactions and correlations between different transaction sets, accounts, names, addresses and other similar information. The individual may have different accounts in different banks or under different names or have false identification. Making such links between transactions on all related
accounts, or by the same or related individuals is important. Then, after finding suspicious activities, the investigators trace the assets and conduct further investigations to identify the origin of the money [158].

A simple understanding of how AUSTRAC investigates money laundering activities could be as illustrated in Figure 2.5 below:

![Diagram of AUSTRAC investigation process]

**Figure 2.5 Example of how the investigation of money laundering works in Australia**

**Reporting requirements and SARs**

In **Australia**, the Financial Transaction Reports Act 1988 (FTR Act) establishes reporting requirements for cash dealers such as banks, credit unions, insurance companies, currency and bullion dealers [189]. Cash dealers in Australia are required to produce the following three types of reports:

- Significant cash transactions of AUD 10,000 or more
- Suspicious transactions reports
- International funds transfer instructions regardless of value.

Additionally, Div 1A of the FTR Act requires the public to report transfers of currency into or out of Australia of AUD 10,000 or more. Div 1B of the FTR Act requires solicitors to report significant cash transactions of AUD 10,000 or more. Moreover, the FTR Act was supplemented by the Federal Parliament by the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act). With regard to the UAE, the Federal Law No. 4 of 2002 requires all financial and commercial institutions to report suspicious activities to the AMLSCU.

---

6 or its equivalent in other currencies.
The UAE regulations require the declaration of cash when importing cash into the UAE of AED 40,000 or more (approximately USD 10,900). Additionally, the security markets and their brokers are required by the UAE regulations to record transactions of AED 40,000 or more and to verify the identity of the investor [190].

The Proceeds of Crime Act 2002 of the UK requires reporting entities to submit suspicious activity reports [191]. In June 2007, the UK applied the European Parliament and Council Regulation (EC) No 1889/2005 on controls of cash entering or leaving the European Union. The Control of Cash (Penalties) Regulations 2007 of the UK requires the public to declare carrying cash of a value of 10,000 Euros or more, or its equivalent in other currencies, when entering or leaving the UK [192].

In the USA, the Bank Secrecy Act regulations require financial institutions to submit the following types of reports [193]:

- Currency transaction report in excess of USD 10,000
- Suspicious activity report
- Report of international transportation of currency or monetary instruments of USD 10,000 or more into or out of the USA
- Report of financial bank and accounts exceeding USD 10,000 in a calendar year.

The reporting of suspicious transactions is considered an essential element in combating money laundering [181, 182]. The data collected from suspicious transactions reports (SARs) helps law enforcement agencies in detecting and investigating money laundering. Therefore, it is important for the reporting entities in each country to determine whether the transactions or activities reflect suspicious possibly illegal activities or not. The FATF [194] indicated that:

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

In Australia, the Financial Transaction Reports Act 1988 has similar provisions on the types of suspicious transactions. Div 2(16) of the Act indicates that:
a cash dealer is a party to a transaction; and the cash dealer has reasonable grounds to suspect that information that the cash dealer has concerning the transaction: (i) may be relevant to investigation of an evasion, or attempted evasion, of a taxation law; or (ii) may be relevant to investigation of, or prosecution of a person for, an offence against a law of the Commonwealth or of a Territory; or (iii) may be of assistance in the enforcement of the Proceeds of Crime Act 1987 or the regulations made under that Act; or (iv) may be of assistance in the enforcement of the Proceeds of Crime Act 2002 or the regulations made under that Act...

Article 7 of the UAE Federal Law No. 4 of 2002 indicates that all financial institutions and other financial, commercial and economic establishments shall submit suspicious transaction reports. The law does not specify what are reasonable grounds to deem transactions as suspicious or not.

Section 330 of the UK Proceeds of Crime Act 2002 mandates obligation on the regulated sector to submit suspicious activity reports as follows:

(1) A person commits an offence if each of the following three conditions is satisfied. (2) The first condition is that he (a) knows or suspects, or (b) has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering. (3) The second condition is that the information or other matter (on which his knowledge or suspicion is based, or (b) which gives reasonable grounds for such knowledge or suspicion, came to him in the course of a business in the regulated sector. (4) The third condition is that he does not make the required disclosure as soon as is practicable after the information or other matter comes to him.

The USA Department of Treasury, the Comptroller of the Currency, and other federal bank regulators, implemented some regulations concerning the reporting of suspicious activity. Under Title 12 of the Code of Federal Regulations, Part 21, banks shall file a suspicious activity report and send it to FinCEN in the following circumstances [195]:
(1) Insider abuse involving any amount. (2) Violations aggregating $5,000 or more where a suspect can be identified. (3) Violations aggregating $25,000 or more regardless of potential suspects. (4) Transactions aggregating $5,000 or more that involve potential money laundering or violate the Bank Secrecy Act.

In contrast to the USA, Australia, the UAE and the UK have no minimum thresholds if there are some reasonable grounds for treating the transaction as suspicious. The UAE legislation does not specify what types of activities that could be considered suspicious transactions. These differences between the four countries in having different interpretations of the types of suspicious transaction, would be expected to affect some variations in the number of SARs.

2.4 Limitations of the Existing Approaches

This section discusses the problems facing countries in combating computer crime and cybercrime. This section discusses the following limitations, challenges and issues:

- Legislation and jurisdiction
- Policy and procedures
- Technology and staff resources
- Computer crime and statistics.

2.4.1 Legislation and Jurisdiction

There has been much research on the development of harmonized computer crime cybercrime legislation around the world. Therefore, legislation that addresses computer-related crime is under continual development even in developed countries. In 2007, Lord Broers [196], the head of the Personal Internet Security sub-committee for the House of Lords, said that the UK may introduce new anti-cybercrime legislation. He added that one of the proposals was for establishing a computer crime complaints centre based online [196]. In 2009, the International Telecommunication Union (ITU) [62] indicated that:

*Today, although every country on the planet is connected to the Internet, many of them do not have a cybercrime law, and among those that do,*
the conflicts and inconsistencies in the laws make it difficult or impossible to investigate, prosecute, and punish cyber criminal behavior. 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 many countries have introduced legislation to combat computer crime and cybercrime, many other countries do not have legislation to criminalize misuse and abuse of computer systems [1]. As a result, it is very difficult sometimes to prosecute criminals when no laws or no cooperation exist between countries. A good example of this issue is the Philippine hacker who launched in 2000 a virus called the “Love Letter” virus [1]. The virus spread throughout the world and the estimated damage in the USA alone was in billions of dollars [1]. However, the USA or the Philippine government could not prosecute the hacker because at that time there was no law in Philippine that criminalises unauthorised access to computer systems [1]. For that, without having laws and cooperation in place, multi-jurisdictional crimes still pose a real issue for law enforcement agencies around the globe. Therefore, in 2006, Interpol called on countries to assist the law enforcement agencies in prosecuting cyber criminals by making it easy for evidence to be transferred between them [197]. Jurisdiction presents a very complicated and real issue when investigating international multi-jurisdiction computer crime [198, 199]. The Committee on Science and Technology of the UK Parliament indicates in their 2006 report that the mechanisms for international cooperation between law enforcement agencies are inefficient and slow-moving [148].

In February 2008, the French Internal Affairs Minister [200] announced new measures for combating cybercrime that included “extending the websites blacklist and pushing for computer online investigations, without the permission of the country of the hosting company”. The last measure could create some challenges and issues, because how can French law enforcement agencies conduct an online investigation without permission from the country that hosts the investigated website. Indeed, the French government suggested these measures to the EU member countries[200].
In 2001, and as indicated in Section 2.2.1, the UN members rejected a proposal for a global cybercrime treaty [63]. They could not reach an agreement on some issues such as transferring of digital evidence and that such a treaty would take a long time to resolve.

### 2.4.2 Policy and Procedures

Even in some developed countries, prosecution of computer crime or cybercrime is still not a high priority for police work [201]. Nancy Ritter, a writer and editor at the USA’s NIJ wrote in 2006, that there is a need for establishing standards for collection and analysis of digital evidence and to produce consistent standards for the certification of examiners [202]. More recently, the UK government has produced guidelines that address some of the researchers’ concerns such as in order to prosecute the owner of a dual use tool it needs to identify that they intended to use it to perpetrate computer crime [92]. Conversely, the guidelines have not discussed the distribution of such a dual use tool; therefore, it is still possible to prosecute the person who distributes such tools [92]. Microsoft has mentioned [148, 201] that there are no particular reporting mechanisms being used in the UK as in the USA. In fact, the UK London’s Metropolitan Police Service reported in 2007 that [33] the reporting and investigating computer crime are key challenges for law enforcement.

### 2.4.3 Technology and Staff Resources

The Committee on Science and Technology of the UK Parliament noted [148] that “there are huge technical challenges in investigating e-crimes. The examination of IT equipment, hard disks, mobile phones or other devices, is highly specialised, time-consuming and resource-intensive”. In addition, the encryption is a difficult problem which faces the computer crime or cybercrime investigators [198]. The UK London’s Metropolitan Police Service reported in 2007 that [33] the “policing of e-crime faces the challenges of keeping pace with technological advances”.

Furthermore, the UK London’s Metropolitan Police Service reported on the 25th of January 2007 that “specialist e-crime units can no longer cope with all e-crime” [33]. Currently most crimes involve the use of computer systems, either as a tool or repository. Therefore, transferring all crime involving the use of computers to
the specialist unit in computer crime will create a huge load when it may not be required. London’s Police added in their report that the “ability of law enforcement to investigate all types of e-crime locally and globally must be ‘mainstreamed’ as an integral part of every investigation, whether it be specialist, or murder, robbery, extortion demands, identity theft or fraud” [33]. Paul Kurtz (Kerbs, 2007), a former White House cyber security adviser for the Bush Administration, said that [144]:

*The FBI – for what resources it has – is not doing a bad job. But when we have as many problems going on as we have today, with China and Russia and organized crime and white-collar criminals getting involved in computer crimes, we don’t have nearly enough agent workforce to take on this problem. And until we see a major increase, we’re going to remain behind on fighting this problem.*

Kshetri [1] wrote in 2006 that the local police forces in most countries are not capable of dealing with the global nature of computer crime or cybercrime. A senior official from the USA I3C reported in 2004 that the FBI has been unable to employ and keep the best available IT experts [1]. Indeed, in 2006, Bhaskar mentioned that “there are simply not enough law enforcement officers at the state level with appropriate computer forensics and computer crime investigative skills” [203]. On the public level, some home and business users are not adequately aware of how to protect their systems [104].

### 2.4.4 Computer Crime and Statistics

According to the EU, some types of computer crime or cybercrime have become regular occurrences. These types include web site defacement, organised fraud, fraudulent transactions, computer hacking, computer viruses, high-tech crime, identity theft and all types of computer fraud [66]. In the Cooperation against Cybercrime Conference [204], organised by the CoE Convention on Cybercrime, that was held in Strasbourg on 11-12 of June 2007, discussions were included on particular web-based threats. Some of the threats that were discussed in the conference include: malicious codes and software, spam emails, botnets, adware and spyware, sexual exploitation of children, and online fraud [204]. In 2006,
Christopher Painter, deputy chief of the USA Department of Justice’s Computer Crime and Intellectual Property Section answered a question about what are the greatest threats right now, with this response [205]: “Phishing continues to evolve in different ways. Botnets still are the hot ticket. Zero-day vulnerabilities are certainly a concern”. In 2007, Interpol outlined some of the threats that face computer and network systems. These threats include [74]: attacks against computer data and systems, Internet auction fraud, child sexual abuse and identity theft. Besides that, there is a concern from growing threats of Botnets through the Internet [75].

With regard to recording computer crime in the UK, only the offences that are criminalised by the Computer Misuse Act 1990 are classified and recorded under the computer crime category, the other crimes that involve computers are not recorded with them [104]. As a result, producing statistics about the scale of computer crime in the UK is difficult. Kshetri [1] wrote in 2006 that there is no cyber criminal database that exists within law enforcement agencies which obstructs their capability to solve such crimes. One of the estimations hints that only 17% of organisations report losses from cybercrime to law enforcement [1]. Many victims do not report computer crime for reasons such as the fear of losing trust [1]. In 2007, the UK London Metropolitan Police Authority [33] wrote in their report that “measuring the extent of e-crime within London and/or affecting Londoners and the UK is a huge challenge due to its global, borderless character”.

Lyons, a security consultant who used to work with the UK’s National Hi-Tech Crime Unit said that the “Law enforcement is only able to take on the top three percent of four percent of the most serious crimes”. In November 2007, MacAfee, the computer security company, warns that there is no end in sight to the work on combating cybercrime [206]. Anthony Adamski, the FBI chief of the financial crimes unit, said that the FBI has only recently commenced to keep computer crime statistics [207].

**2.4.5 Summary**

This section has discussed the limitations, challenges and issues that are facing law enforcement agencies concerning countering cybercrime. It indicates the need for more work to be done in order to have better approaches regarding combating
computer and cybercrime. One way of doing this is through conducting in-depth research in this field.

## 2.5 Research Methodology

Despite the extent of cybercrime and its continued rapid increase, the approaches for combating computer crime, including money laundering, are not uniformly well established. This impedes efforts to identify and report accurately on the exact extent of the problem, and consequently how best to combat the problem. The purpose ultimately is to identify areas where improvements are needed and what those improvements should be.

The thesis is intended to answer the following overall research question:

*Given the serious and global nature of computer crime and taking into account varying cultural differences and influences, is there internationally a sufficient understanding of it and a sufficiently consistent approach for dealing with it effectively, and what improvements are needed?*

As indicated in Chapter 1, the research presented in this thesis has a number of themes, and the above overall research question is refined to four more detailed research questions which focus on those themes. Each of these four questions is addressed by one chapter of the thesis.

In this section we pose each question in turn, and then follow each question by describing the methodology we have used to address the question.

**Q1.** *To what extent are the current definitions and taxonomies of computer crime and current computer crime or cybercrime legislation appropriate for the effective investigation and prosecution of cybercrime in the international context and what improvements are needed?*

This research question needs to be further refined to the following two:

**Q1(a)** *To what extent are the current definitions and taxonomies of computer crime appropriate to the accurate and consistent reporting internationally of computer crime and its prosecution and what improvements are needed?*

This question is addressed by Chapter 3. It examines and analyses the variety of terms and definitions used to describe computer crime and investigates
different computer crime taxonomies that are in use or have been proposed. The chapter then proposes a unified comprehensive taxonomy of computer crime.

**Q1(b)** To what extent does the computer crime or cybercrime legislation in Australia, the UAE, the UK and the USA differ and to what extent is that legislation in alignment with the Council of Europe (CoE) Convention on Cybercrime and what improvements are needed in this regard?

This question too is addressed by Chapter 3 which discusses the computer crime and cybercrime Legislation in Australia, UAE, the UK and the USA. The purpose of Chapter 3 is to answer the research questions 1(a) and (b). Ch 3 comprises a comparative analysis of computer crime or cybercrime legislation enacted in Australia, the UAE, the UK and the USA that aligns with the CoE Convention on Cybercrime. The intention is to reveal how the legislations in these countries align with the criminal provisions provided under Articles 2 to 11 of the Convention. In doing this, Chapter 3 makes use mainly of the CoE Convention on Cybercrime [20] and its Explanatory Report [208], in addition to the legislation enacted in Australia, the UAE, the UK and the USA. While it is important to cover every article of legislation for each country, the study is limited to covering the federal legislation for the purpose of comparing how they align with the Convention. Additional information that is made available by the government websites of these countries and information made available through other sources, both academic and non-academic, are included for the purpose of illustration when it is needed.

With regard to Articles 2 to 11 of the CoE Convention on Cybercrime, each Article is analysed to identify its main provisions. Then, an analysis is presented of how the computer crime or cybercrime legislation is enacted in Australia, the UAE, the UK and the USA to resolve the criminal provisions identified under Articles 2 to 11. The analysis identifies how each country’s legislation aligns with each of the Articles 2 to 11. Chapter 3 ends with identification of a new framework to develop harmonised computer crime or cybercrime legislation globally.

**Q2.** To what extent are the approaches for combating computer crime in Australia (as represented by the QPS) and the UAE (as represented by the ADP) different and what improvements are needed?
The purpose of Chapter 4 is to answer this second research question. This question too is further refined in terms of the following three propositions:

**Proposition 1:** The legislation used in Queensland to counter computer crime is different to that used in Abu Dhabi.

**Proposition 2:** The policy, procedures, technology and staff resources used in Queensland to counter computer crime are different to those used in Abu Dhabi.

**Proposition 3:** The nature and extent of computer crime or cybercrime in Queensland is different to that in Abu Dhabi.

The research described in this chapter used a qualitative research method focusing on two major case studies. The first case study is the Abu Dhabi Police (ADP), and the second is the Queensland Police Service (QPS). After negotiating with both the ADP and QPS, the researcher obtained permission to conduct a written questionnaire and follow-up interviews with participants from the above mentioned police forces. 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.

According to Yin [209], there are five ways to do social science research: experiments, surveys, histories, analysis of archival information, and case studies. Yin indicated that each one has advantages and disadvantages based on three conditions: “(a) the type of research question, (b) the control an investigator has over actual behavioral events, and (c) the focus on contemporary as opposed to historical phenomena” [209]. Generally, the methodology of this thesis is considered exploratory, descriptive and comparative in order to identify and compare the approaches used by Australia and the UAE for combating computer crime.
A case study approach can be used to answer the research questions and this approach can be viewed, studied and analysed alone (within-case analysis) or compared to other cases (cross-case analysis) to provide comparison and contrast rich detail and insights regarding the research issues [210-212]. When dealing with multiple case studies, it is important to “provide a detailed description of each case and themes within the case, called a within-case analysis, followed by a thematic analysis across the cases, called a cross-case analysis, as well as assertions or an interpretation of the meaning of the case” [213]. Accordingly, the analysis of the data has been done in three parts. Firstly, the ADP data has been analysed using within-case analysis. The aim was to present emerging themes and patterns from the ADP data. The themes and patterns helped to find out the key findings and main contributions. Secondly, the QPS data was analysed using a within-case analysis. Finally, the cross case analysis of both cases, ADP and QPS, focuses on the comparisons between the two cases through looking at and summarizing the similarities and differences between them. The point of focus within the ADP and the QPS is on particular police units which are particularly responsible for combating cybercrime. In relation to the ADP, the focus is on the Computer Crime Unit and in terms of the QPS, there are four police units: Computer Crime Investigation Unit (CCIU), Identity Crime Unit (IDCU), Proceeds of Crime Unit (PoCU), and Forensic Computer Examination Unit (FCEU). The four QPS units involved in this particular area of criminal investigation operate under the Fraud and Corporate Crime Group/State Crime Operations Command.

Administering written questionnaires and interviewing are the most generally used case study research techniques [214]. Written questionnaires are sometimes useful in small scale studies on sensitive areas [214]. Face-to-face interviews with respondents can help provide a depth of understanding and information in several qualitative areas [215]. The interview sometimes is valuable as a follow-up to respondents’ answers and to further study the responses [216].

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 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. 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 the nature of 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 obviously incorrect responses 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 objectives in order to answer the second research question.

Testing the above three propositions should provide valuable insight into the above research question. In pursuing that aim, the propositions guided the creation of the questionnaire and interview questions. The questions were developed and structured into three different categories. These categories are: legislation and jurisdiction; policy, procedures and resources; and the nature and extent of computer crime. The first category, legislation and jurisdiction, consists of the legislation and jurisdiction themes. The second category includes 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. The last category is about the nature and extent of computer crime theme.

Q3. To what extent does the extent of money laundering in Australia, the UAE, the UK and the USA differ and how has it changed over time?

The purpose of Chapter 5 is to answer the above research question. In order to achieve its aim, this chapter makes use of money laundering and related statistics in Australia, the UAE, the UK and the USA. This chapter also presents and analyses information made available by the government websites of these countries and information made available through other sources, both academic and non-academic.

Q4. To what extent do the anti-money laundering/combating financing of terrorism regimes in Australia, the UAE, the UK and the USA differ with respect to
their compliance with the international Financial Action Task Force (FATF) recommendations and to what extent have local factors, such as cultural and economic factors, affected the UAE's compliance with these recommendations and what improvements are needed?

The aim of Chapter 6 is to answer the fourth research question. It focuses on identifying how the AML/CFT regimes of Australia, the UAE, the UK and the USA have interpreted and remained faithful to the FATF recommendations, and whether compliance with the FATF recommendations is affected by local factors in these countries, factors such as economic and cultural factors. Therefore, this chapter makes use of the FATF evaluation reports for Australia, the UAE, the UK and the USA to compare their compliance and to analyse how they have interpreted and remained faithful to the FATF recommendations. It also uses other sources including government documents, international organisations’ documents, and academic and non-academic in order to carry out the research.

2.6 Conclusion

Cyber criminals have benefited from the computer and Internet's technology to commit their crimes. Computer crime or cybercrime can be defined broadly as a crime that utilises or targets computer data and systems for committing an illegal activity. Indeed, governments and international organisations are working on introducing tougher laws to reduce the incidence of computer crimes. Therefore, any research into the approaches and practices for combating computer crime is a significant work that could help identify the most effective approaches for combating such criminal activity.

The aim of this chapter was to study the approaches of countering computer crime. The first section commenced with the discussion on the definitions of computer crime or cybercrime, taxonomy of computer crime and cybercrime and the global extent of computer crime and cybercrime. Then, the second section reviewed the national and international approaches for combating computer crime including computer crime and cybercrime legislation, government initiatives, and law enforcement approaches. Section 2.3 examined the approaches used in Australia, the UAE, the UK and the USA for combating money laundering.
The review of the literature revealed some existing limitations of the approaches to and practices for combating computer crime, which were discussed in Section 2.4.

In conclusion, this literature review described several approaches and practices for combating computer crime or cybercrime. However, the limitations, challenges and issues which have been identified through the literature, indicated a clear need to improve existing approaches to enhance the capabilities of law enforcement agencies in combating computer-related crime. This is the focus of this thesis.

Chapter 3 proposes a unified comprehensive taxonomy of computer crime that identifies how computer crime may be classified based upon the dual characteristics of the role of the computer and the contextual nature of the crime. It also reveals how the legislation in the Australia, the UAE, the UK and the USA align with the criminal provisions provided under Articles 2 to 11 of the Convention.
Chapter 3

Chapter 2 examined and analysed the nature of computer crime and existing international approaches used for combating such crime. This chapter is motivated by the need to enable accurate and consistent reporting of cybercrime, an essential pre-requisite for informed monitoring and combating of the critical problem that computer crime or cybercrime poses to developed and developing economies. Chapter 3 also comprises a comparative review of the federal cybercrime legislation enacted in Australia, the UAE, the UK and the USA that corresponds to the CoE Convention on Cybercrime (CoE Convention). The aim is to reveal how legislation in these countries corresponds with the criminal provisions provided under Articles 2 to 11 of the CoE Convention. Chapter 3 aims to identify the existence of computer crime laws that address the criminal offences identified under Articles 2 to 11 of the CoE Convention and to develop a preliminary analysis of the degree of alignment of the legislation with those Articles.

The CoE Convention is considered to be the most important international guideline that has been developed to combat computer-related crime. The CoE Convention currently only applies to members of the European Union although other jurisdictions have adopted some aspects of the Convention. There have been previous research studies conducted to understand how individual countries align with the CoE Convention. Urbas (2001) [217] compares the cybercrime legislation enacted in the Asia-Pacific Region (including Australia) to the criminal provisions of the CoE Convention. Urbas found that some of the cybercrime legislation which

was enacted in the Region overlaps with other criminal, commercial and intellectual property laws. Picotti and Salvadori (2008) [218] analysed and compared the cybercrime legislation enacted in 24 European and nine non-European countries to the CoE Convention. Their analysis did not include detailed considerations of computer crime or cybercrime legislation enacted in Australia, the UAE, the UK or the USA. Therefore, this thesis contains a detailed review, analysis and comparison of the legislation in these four countries corresponding to Articles 2 to 11 of the CoE Convention.

This chapter makes use mainly of the CoE Convention [20] and its Explanatory Report [208], in addition to the federal legislation enacted in Australia, the UAE, the UK and the USA. Additional information that is made available by the government websites of these countries and information made available through other sources, both academic and non-academic, are included for the purpose of illustration when it is needed.

Overall, Chapter 3 aims to address the following research question:

Q1. To what extent are the current definitions and taxonomies of computer crime and current computer crime or cybercrime legislation appropriate for the effective investigation and prosecution of cybercrime in the international context and what improvements are needed?

In order to answer this question, we focus more on two specific questions:

Q1(a) To what extent are the current definitions and taxonomies of computer crime appropriate to the accurate and consistent reporting internationally of computer crime and its prosecution and what improvements are needed?

Q1(b) To what extent does the computer crime or cybercrime legislation in Australia, the UAE, the UK and the USA differ and to what extent is that legislation in alignment with the Council of Europe (CoE) Convention on Cybercrime and what improvements are needed in this regard?

The first section of the chapter, Section 3.1, proposes a unified comprehensive taxonomy of computer crime that identifies how computer crimes may be
classified based upon the dual characteristics of the role of the computer and the contextual nature of the crime. Section 3.1 addresses the research question Q1(a). Section 3.2 consists of a comparative review of the cybercrime legislation enacted in Australia, the UAE, the UK and the USA that correspond to the CoE Convention. Section 3.2 also discusses the findings of this research and addresses the research question Q1(b). The third section (3.3) proposes a new framework to develop harmonised computer crime or cybercrime legislation globally. Section 3.4 summarises the findings of this chapter.

Several of the results presented in this chapter have been published in the following conference paper:


### 3.1 A Model for Classifying Computer Crime

This section presents the development of a systematic and comprehensive taxonomy of computer crime based not only upon the role of the computer, but also on the contextual information surrounding the crime such as motive and offender’s relationship. The first sub-section (3.1.1) highlights the need for a consistent taxonomy of cybercrime and consistent definitions to assist with communication and cooperation between commercial and government organisations and to assist with the harmonisation of regulation and legislation across organisational and jurisdictional boundaries. Sub-section 3.1.2 refines the Role I and II (or Type I and II) classification of computer crime, which was discussed in Chapter 2, into a number of sub-types and uses that refined classification scheme or taxonomy to categorise a comprehensive list of common computer crimes and cybercrimes. Sub-section 3.1.3 presents the case for a taxonomy which is extended further still to incorporate contextual information such as main motive/offender role, the offender relationship and scope of impact, as well as the role of the computer. Sub-section 3.1.3 then presents a detailed analysis of a number of significant computer crime case studies and classifies them

---

7 The term ‘computer’ in this thesis denotes any digital device including a computer system.
according to this extended taxonomy, presenting a summary in table form to illustrate the expressiveness of the proposed extended taxonomy. The fourth sub-section (3.1.4) proposes a universal classification code for categorising computer crime. Sub-section 3.1.5 maps the CoE Convention to the proposed computer crime classification in Sub-section 3.1.2.

3.1.1 The Need for a Consistent Taxonomy of Computer Crime

Grabosky, Smith and Dempsey [219] note that the “fundamental principle of criminology is that crime follows opportunity, and opportunities for theft abound in the Digital Age”. Grabosky [220] indicates that the growth of computer technology and the Internet have increased the opportunities for criminals to commit computer crime or cybercrime. Also, Broadhurst (2006) [221] indicated that the transnational nature of computer crime or cybercrime reflects its position as a global problem. While, the problem of computer-related crime has been known and identified for sometime now, there are markedly different interpretations of the nature of computer crime or cybercrime [11]. This has resulted in a wide range of computer crime or cybercrime definitions and taxonomies. Some types of crimes that involve the use of computers may or may not be considered to be computer crime or cybercrime depending on the organisation involved and the type of categorisation used. For example, an offence might be a crime or computer crime in one country and not in another. Such problems have resulted in difficulties in reporting, monitoring and comparing the scale of computer crime between different jurisdictions. In fact, Broadhurst (2006) [221] noted that “in many jurisdictions cyber-crimes, if reported, may be not be differentiated from other commercial crime, fraud reports or criminal damage statistics or other categories”. For instance, Scott Charney from Microsoft noted at the AusCERT 2008 conference that they have found problems in judging the extent of computer fraud because it is not considered as computer crime in some jurisdictions [222]. Such variations have resulted in difficulties in reporting and comparing the scale of computer crime between countries. To complicate matters still further, some law enforcement agencies associate the term cybercrime specifically with cases that involve complex computer-specific issues, or cases that require computer forensic examination such as computer hacking [41].
One reason that it is important to attempt to develop a more detailed taxonomy of computer crime with agreed definitions is so that investigators and agencies, regardless of their location, affiliation and jurisdiction can investigate, communicate and cooperate with each other using consistent interpretation, approaches or practices. In fact, the UN [49] noted that the problems surrounding international cooperation in the area of computer crime include both the lack of global agreement on what types of conduct should be designated as computer crime and on the legal definition of criminal conduct. Without common agreement or understanding on computer crime or cybercrime definitions and taxonomy, it is difficult to report on its nature and extent consistently from one country to another. Furnell (2001) [11] 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 [50] has recommended each country to map its high-tech crime taxonomy to “make it addressable with other countries” and extend it to “take into account ICT or ‘high technology’ use and/or activity (for instance cell phones fraud, remote bomb priming)”.

To summarise: the adoption of consistent computer crime or cybercrime definitions and a consistent taxonomy is needed in order to assist in the following activities:

- sharing information
- reporting and accurate monitoring of computer crime cooperation and collaboration
- cooperation on combating computer crime.

Finally, the acceptance of common computer crime definitions and a common taxonomy will assist progress in harmonising computer crime and cybercrime regulation and legislation.

### 3.1.2 The Refined Type I/II Model - Refining the Role I and Role II Classification of Computer Crime

The purpose of reviewing and investigating different definitions and classifications of computer crime is to develop a consistent and comprehensive taxonomy that
will benefit the organisations that deal with combating such crimes. Some of the benefits include: sharing of information, accurate reporting of cybercrime cases, informed monitoring of the scale of the problem, cooperation on actual cases, cooperation on combating cybercrime, and harmonisation 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 [49]. The CoE computer crime taxonomy is a broader classification for offences involving the use of computers [20]. However, the CoE cybercrime classification too does not include a number of other types of crimes that are supported or facilitated through the use of computers such as identity theft. The G8 classification of computer-related crime, focuses on the types of threats to computer and computer systems rather than crimes in general [50].

Chapter 2 has reviewed and analysed various computer crime or cybercrime definitions and classification schemes, currently in use or proposed. Based on our studies, we have further below consolidated a comprehensive list of crimes that are generally regarded as computer crime and classified them according to the Role I and Role II classification outlined in Chapter 2. For the purpose of this thesis, we will refer to computer crime in which the computer has Role I or Role II as Type I or Type II computer crimes respectively. We have extended the Type I and Type II classification by identifying different sub-types for both Type I and Type II offences. These sub-types appear to us to be intuitive and enable us to arrive at a natural classification of the list of computer crimes. Some of the previous work on classifying computer crime or cybercrime reviewed in Section 1 of Chapter 2 has likewise been extended to include sub-types but that work has either by-passed the major Type I and II classification (e.g., CoE [26]) or 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-types borrow from and consolidate some of that previous work to provide a more comprehensive and expressive model. We will refer to this Type/Sub-type classification henceforth as the refined classification.
**Type I sub-types**

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

A. *Unauthorised access offences* [49] such as hacking
B. *Malicious code offences* [50] such as the dissemination of viruses and worms [39]
C. * Interruption of services offences* [41] such as disrupting or denying computer services and applications e.g., denial of service attacks and Botnets
D. *Theft or misuse of services* [32, 44]: examples of theft or misuse of services include theft or misuse of someone’s Internet account or domain name [41].

**Type II sub-types**

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-types:

A. Content violation offences [32] such as the possession of child pornography, unauthorized possession of military secrets, IP offences
B. Unauthorised alteration of data, or software for personal or organisational gain [223] such as online fraud
C. Improper use of telecommunications [39] such as cyber stalking, spamming, and the use of carriage service with the intention or conspiracy to commit harmful or criminal activity. Also it covers social engineering fraud such as phishing and scareware [224].

We present this refined taxonomy and a list of common examples of computer crime classified according to the refined taxonomy in Figure 3.1. It is clear that in some of these crimes, the computer plays dual roles and hence the one crime can be classified under dual types, however there will typically be one primary role, and hence one primary computer crime type classification by which to classify the crime. As a result, the categories of Figure 3.1 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 [35], the USA 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 [225] 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”. This would seem to fit the Type I classification. According to the UK Parliamentary Office of Science and Technology [104], 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”. This implies a Type II crime. Indeed, the Australian High Tech Crime Centre [43] categorised cyberterrorism under Type II along with fraud, money laundering and other traditional crimes. Others [35] have considered physical attacks (not using a computer) against critical infrastructure such as the Internet, telecommunications, and the electric power grid as cyberterrorism.

It seems evident that any attack against a computer and computer network that is intended for political purposes is a computer crime or cybercrime and can be labelled as cyber-terrorism and Urbas and Choo [44] have indeed categorised cyberterrorism-related offences under Type I. In fact, any offence that comes under computer crime Type I could be considered cyberterrorism if the intent of the attacker was to commit a terrorism act. The FEMA [35] and Coleman [225] definitions of cyber-terrorism indicate that some computer crime or cybercrime Type II offences can be considered cyber-terrorism, depending upon the intent of the attacker (e.g., theft of military secrets). We note therefore that cyber-terrorism activity 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 computer crime committed in this terrorist act: Type I and Type II.
3.1 A Model for Classifying Computer Crime

Threats (as opposed to actually carrying out the threats) against critical infrastructure fall typically under Type II.

Figure 3.1 Refined computer crime classification

3.1.3 The Extended Refined Model – Extended with Contextual Features

The question to be asked at this point is how accurately and completely does the above refined Type/Sub-type classification, illustrated in Figure 3.1, depict actual cases of computer crime? This classification based on identifying the type of 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 the scope of impact. Identifying such additional markers promises to be important for government and international bodies who work in the area of crime trending and analysis, and who set strategies to counter and prevent such crimes. We therefore focus in this sub-section on analysing a range of computer crime cases in detail, including not just the type of computer crime in terms of (the refined)
Types I and II, but also contextual information regarding main motive/offender role, the offender relationship, and the scope of impact. We refer henceforth to this classification as the *extended taxonomy*. In analysing these cases, we assessed the following characteristics of each offence:

- *The type of computer crime*: which type or types of computer crime have been committed (computer crime Type I/II)
- *Sub-type classification*: where does each offence appear in the refined classification represented in Figure 3.1
- *Main motive/offender role*: what are the motives of the offence; is it an individual’s motives, or is it 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 analysed the following well-known computer crime case studies according to the refined Type I/II classification scheme and contextual markers identified above:

- Morris worm [226]
- Maroochydore public waterways sewage [227]
- Harassment letter send by email
- USA v. Gorshkov & USA v. Ivanov [228, 229]
- Fungible credentials [230]
- International Interpol-led investigation on child pornography [231]
- ShadowCrew [232]
- Holiday prize scam [233]
- Fraud and money laundering scheme [234].

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. Appendix A presents our detailed analysis of each case, and
Tables 3.1 and 3.2 present a summary of those analyses. The summaries in Table 3.1 and Table 3.2 capture the essential features of the crimes analysed and provide a concise but sufficient description of each crime to enable informed reporting and an accurate statistical analysis of the nature of the computer crime or cybercrime involved. We believe this demonstrates the applicability and utility of the extended refined taxonomy.

Table 3.1
Discussion of some computer crime case studies

<table>
<thead>
<tr>
<th>Case #</th>
<th>Case name/detail</th>
<th>Type of computer crime</th>
<th>Refined classification (Fig. 3.1)</th>
<th>Main motive/offender role</th>
<th>Offender relationship</th>
<th>Scope of Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Morris worm</td>
<td>Type I</td>
<td>I.B2, I.C1</td>
<td>individual</td>
<td>outsider</td>
<td>Business, government and the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Maroochydore public waterways sewage Harassment letter send by email</td>
<td>Type I</td>
<td>I.A1</td>
<td>individual</td>
<td>outsider</td>
<td>Business and government</td>
</tr>
<tr>
<td>3</td>
<td>USA v. Gorshkov USA v. Ivanov</td>
<td>Type I and Type II</td>
<td>I.A1, II.B2, II.C5, II.C6,</td>
<td>Individuals and organised crime</td>
<td>outsider</td>
<td>Business</td>
</tr>
<tr>
<td>4</td>
<td>Fungible credentials International Interpol-led investigation on child pornography</td>
<td>Type II</td>
<td>II.A7</td>
<td>Individuals and organised crime</td>
<td>outsider</td>
<td>Individuals</td>
</tr>
<tr>
<td>5</td>
<td>Shadowcrew</td>
<td>Type I and Type II</td>
<td>I.A1, I.D1, II.B1, II.B2, II.C8</td>
<td>Organised crime</td>
<td>outsider</td>
<td>Individuals and business</td>
</tr>
<tr>
<td>6</td>
<td>Holiday prize scam Fraud and money laundering scheme</td>
<td>Type II</td>
<td>II.B2, II.C8</td>
<td>Organised crime</td>
<td>outsider</td>
<td>Individuals</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td>II.B2, II.C2, II.C5</td>
<td>Organised crime</td>
<td>outsider</td>
<td>Individuals</td>
</tr>
</tbody>
</table>

...
Table 3.2
Characteristics of some computer crime case studies

<table>
<thead>
<tr>
<th>Case #</th>
<th>Case name/detail</th>
<th>Type I Target</th>
<th>Type II Tool</th>
<th>Refined classification (Fig. 3.1)</th>
<th>Main motive/offender role</th>
<th>Offender relationship</th>
<th>Scope of Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Morris worm</td>
<td>√</td>
<td>X</td>
<td>I.A2, I.C1</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>Maroochydore public waterways sewage</td>
<td>√</td>
<td>X</td>
<td>IA1</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>Harassment letter send by email</td>
<td>X</td>
<td>√</td>
<td>II.A1</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>USA v. Gorshkov USA v. Ivanov</td>
<td>√</td>
<td>√</td>
<td>I.A1, II.B2, II.C5, II.C6,</td>
<td>√</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>5</td>
<td>Fungible credentials</td>
<td>X</td>
<td>√</td>
<td>II.A7</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>6</td>
<td>International Interpol-led investigation on child pornography</td>
<td>X</td>
<td>√</td>
<td>II.A1</td>
<td>√</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>7</td>
<td>Shadowcrew</td>
<td>√</td>
<td>√</td>
<td>I.A1, I.D1, II.B1, II.B2, II.C8</td>
<td>√</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>8</td>
<td>Holiday prize scam</td>
<td>X</td>
<td>√</td>
<td>II.B2, II.C8</td>
<td>√</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>9</td>
<td>Fraud and money laundering scheme</td>
<td>X</td>
<td>√</td>
<td>II.B2, II.C2, II.C5</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
3.1.4 A Universal Classification Code for Computer Crime

In this section, we propose a universal classification code for categorising computer crime based upon the work discussed above. This universal code would facilitate cooperation and communication between law enforcement agencies from different countries, cultures and languages that otherwise would be likely to have different interpretations of computer crime or cybercrime. Table 3.3 illustrates a possible starting point for such a system.

To illustrate with an example, we consider the crime of online fraud: II.B.02. When reporting a crime, a law enforcement agency would use the code when communicating with other agencies regardless of the difficulties encountered in translating or due to varying jurisdictions and their interpretation.

This codification system can then accommodate the additional contextual features proposed in section 3.1.3 above:

- main motive/offender role - [1) individual(s), 2) political, 3) terrorism, 4) organized crime]
- offender relationship to the victim - [1) insider or 2) outsider]
- the scope of impact - [1) global infrastructure, 2) government agency, 3) business, 4) individual(s)].

For example, the second computer crime case study in Table 3.1, the Maroochydore public waterways sewage, would be codified as follows:

I.A.01 (individual, outsider, business and government) – the code ‘I.A1’ refers to the offence of unauthorised access or computer hacking, and is followed by the contextual tags: main motive/offender role: individual; offender relationship: outsider; the scope of impact: business and government.

The codification system that we propose and present in this sub-section is not complete. It is intended as a starting point and to prompt further work on a consistent codification of computer crime and cybercrime in order to assist in cooperation against the threat of such criminal activity.
### Table 3.3
Universal code for the types of computer crime

<table>
<thead>
<tr>
<th>Computer crime type</th>
<th>Main categories under the type</th>
<th>Specific types of computer crime</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type I</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer is the target of criminal activity</td>
<td>A. Unauthorised access</td>
<td>Hacking e.g., unauthorised copying, modifying, or deleting computer data and programs (01)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Viruses (01)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Worms (02)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trojan Horse (03)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software bomb (04)</td>
</tr>
<tr>
<td></td>
<td>B. Malicious code</td>
<td>Disrupting computer services (01)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Denying computer services (02)</td>
</tr>
<tr>
<td></td>
<td>C. Interruption of services</td>
<td>Theft of services (01)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Misuse of services (02)</td>
</tr>
<tr>
<td></td>
<td>D. Theft or misuse of services</td>
<td></td>
</tr>
<tr>
<td><strong>Type II</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer is the tool to commit a crime</td>
<td>A. Content violations</td>
<td>Child pornography (01)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hate crimes (02)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Harmful contents (03)</td>
</tr>
<tr>
<td></td>
<td>B. Unauthorised alteration of data or software for personal or organisational gain</td>
<td>Military secrets (04)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Copyrights crimes (05)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intellectual property (06)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Forgery/Counterfeit (07)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identity theft (01)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Online fraud (02)</td>
</tr>
<tr>
<td></td>
<td>C. Improper use of communications</td>
<td>Privacy (03)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sabotage (incl. critical infrastructure offences) (04)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Telemarketing/Internet fraud (05)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Electronic manipulation of sharemarkets (06)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Harassment (01)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Online money laundering (02)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber stalking (03)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spaming (04)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Conspiracy (05)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Extortion (incl. critical infrastructure threats) (06)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Drug trafficking (07)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Social engineering fraud (e.g. Phishing and scareware) (08)</td>
</tr>
</tbody>
</table>
3.1.5 The CoE Convention and the Refined (Type/Sub-type) Computer Crime Classification

In this sub-section, we aim to illustrate that our proposed Type/Sub-type classification can accommodate any emerging criminal activity or any other computer crime classification. For instance, Table 3.4 below illustrates how the offences identified under Articles 2 to 10 of the CoE Convention can be classified under our proposed classification. Section 3.2 discusses these articles in more detail. Because it does not in itself identify a different type of computer crime, Article 11 regarding attempting and aiding or abetting is not covered in Table 3.4. In some types of the offences identified under the CoE Convention, the computer would play more than one role, yet in such cases, the computer plays one primary role and secondary role, as mentioned in Table 3.4.

Table 3.4
Mapping the CoE Convention to the proposed computer crime classification

<table>
<thead>
<tr>
<th>Computer crime type</th>
<th>Main categories under the type</th>
<th>CoE Convention – Articles 2-10</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type I</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer is the target of criminal activity</td>
<td>A. Unauthorised access</td>
<td>Article 2 – illegal access Article 4 – data interference (PR)</td>
</tr>
<tr>
<td></td>
<td>B. Malicious code</td>
<td>Article 4 – data interference (SR)</td>
</tr>
<tr>
<td></td>
<td>C. Interruption of services</td>
<td>Article 5 – system interference (SR)</td>
</tr>
<tr>
<td></td>
<td>D. Theft or misuse of services</td>
<td>Article 5 – system interference (PR)</td>
</tr>
<tr>
<td></td>
<td>A. Content violations</td>
<td>Article 6 – misuse of devices</td>
</tr>
<tr>
<td><strong>Type II</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer is the tool to commit a crime</td>
<td>B. Unauthorised alteration of data or software for personal or organisational gain</td>
<td>Article 7 – computer-related forgery (PR) Article 8 – computer-related fraud (PR) Article 9 – offences related to child pornography Article 10 – offences related to infringements of copyright and related rights</td>
</tr>
<tr>
<td></td>
<td>C. Improper use of communications</td>
<td>Article 7 – computer-related forgery (SR) Article 8 – computer-related fraud (SR)</td>
</tr>
</tbody>
</table>

Note: PR refers to a primary role; SR refers to a secondary role; of using the computer in a crime.
3.2 Cybercrime Legislation Alignment with the CoE Convention on Cybercrime

This section presents a comparative review of the computer crime and cybercrime legislation used in Australia, the UAE, the UK and the USA as they relate to 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. The section identifies the existence of legislation in these four countries that corresponds to the CoE Convention and the nature of the penalties exacted by the legislation. It also provides a preliminary analysis of the extent to which that legislation aligns with the CoE Convention Articles in terms of the various conditions and additional elements that qualify the provisions of each Article.

Though it is useful to discuss each of these Articles in more detail, the scope of this chapter is limited to discuss Articles 2 to 11 of the criminal law of the CoE Convention. In summary, the articles are as follows:

- 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 attempting and aiding or abetting the commission of any of the offences that are established under Articles 2 to 10.

Appendix B presents the CoE Articles and the detailed results of our analyses as follows: Appendix B.1 presents the actual articles verbatim, Appendix B.2 then discusses each of the articles and Appendix B.3 provides a comparative analysis of the corresponding existing legislation in each of the four countries related to the CoE Convention provisions.

The results of our detailed analysis in Appendix B.3 are presented in Tables 3.5, 3.6 and 3.7. Table 3.5 lists the computer crime legislation in Australia, the UAE, the UK and the USA corresponding to the CoE Articles while Table 3.6 illustrates the
penalties for committing these offences in Australia, the UAE, the UK and the USA. The findings show that Australia, 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 to 11, not all of these offences are criminalised under the one legislation, but rather under different legislations
- All of the four countries provide provisions for the punishment of committing the CoE Convention related offences but 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. Additionally, the UAE criminal sanctions system has smaller and lighter punishments compared to the other countries.

In a further step, we undertook a preliminary analysis of the degree of alignment of the legislation with the Articles as presented in Table 3.7, in terms of the detailed conditions and additional elements that qualify the provisions of each Article. In order to do so, we first identified the various detailed conditions and additional elements qualifying each of the Articles 2 to 11 and present these in Tables B.1 to B.10 of Appendix B.3. In reviewing the legislation of each country we assessed it against these conditions and additional elements and Table 3.7 shows the results of the analysis. It is apparently the case that the degree of alignment with Articles 2 to 11 of the CoE Convention as represented in Table 3.7 is low in Australia and the UK and very low in the UAE.

**Discussion**

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.
Table 3.5 Summary of Australia, the UAE, the UK and the USA legislation corresponding to the CoE Convention

<table>
<thead>
<tr>
<th>CoE Convention</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 6 - Misuse of devices</td>
<td>Cybercrime Act 2001, Criminal Code Act 1995 (Cth): Sections 478.3 and 478.4</td>
<td></td>
<td>Computer Misuse Act of 1990: Section 3A</td>
<td>Computer Fraud and Abuse Act, USA Code Title 18 Sections 1029, 1030 (a)(5)(A) and 2512</td>
</tr>
<tr>
<td>Article 10 - Offences related to infringements of copyright and related rights</td>
<td>Copyright Act 1968 (Cth)</td>
<td>UAE Federal Law No 7 of 2002 regarding Copyright and Related Rights</td>
<td>Copyright, Design and Patents Act 1988</td>
<td>USA Code Title 18 Section 2319, 1030, and 1029 and Title 17: Section 506</td>
</tr>
<tr>
<td>Article 11 - Attempt and adding or abetting</td>
<td>Criminal Code Act 1995 (Cth): Sections 478.3 and 478.4</td>
<td>UAE Federal Law No 2 of 2006: Article 23</td>
<td>Computer Misuse Act 1990: Section 2</td>
<td>USA Code Title 18 Section 1030 (b)</td>
</tr>
</tbody>
</table>
### Table 3.6
Comparison of penalties* for committing computer-related offences identified by the CoE Convention

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

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

Australia and the UK are aligned with seven of 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. This, in fact, evidently shows that the UAE experience in dealing with such crimes is insufficient to develop and implement an adequate criminal law. Nevertheless, on 16 December 2009, the UAE Minister of Justice, Dr Hadeef Al Daheri, noted that the UAE Government was setting up a new Department under their Federal Courts to combat cybercrime [235]. The intention of the department
was to draft new laws and regulations concerning cybercrime, and set plans for prevention mechanisms and 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 Chapter 6 addressing cultural influences on national anti-money laundering legislation.

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 to 11 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 clearly indicates that the UAE legislation is required to be updated to cover some important conditions of the CoE Convention and by extension that there is a need for further progress generally in international harmonisation of cybercrime legislation. This is but one example of argument in support of the ITU’s 2009 plea for international harmonization [62]: “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”.

### 3.3 Proposal to Develop Harmonised Cybercrime Legislation Globally

#### 3.3.1 A New Strategy

While many countries have implemented computer crime and cybercrime legislation and in recent years re-evaluated their cybercrime legislation, there are still nonetheless significant inconsistencies and differences in such laws globally.
Broadhurst (2006) [221] indicates that “[m]any nations and regional bodies such as the CoE have addressed the problem of cyber-crime and laws exist that criminalise unauthorised access and unlawful use of computers, but such laws are neither universal nor uniform”.

The ITU’s recent work and publication in 2009 [62] of the ‘ITU Toolkit for Cybercrime Legislation’ was designed to address this and “provide countries with sample legislative language and reference materials that can assist in the establishment of harmonized cybercrime laws and procedural rules”. The ITU Toolkit was developed after analysing the CoE Convention on Cybercrime and the legislation of developed countries.

Under Section 6, the ITU Toolkit provided a matrix of provisions of leading cybercrime laws of the CoE Convention, Australia, Canada, EU, Germany, Japan, Mexico, Singapore, UK, USA, India and China. The matrix generally illustrates how each country’s law has been used in developing each article of the Toolkit. Though it was a good step forward in harmonisation of cybercrime legislation globally, there are some concerns regarding the use of the applicable law for each computer offence. Overall, we found the following points that raise some concerns regarding the credibility of this Toolkit:

a) The Toolkit indicated in the matrix the use of different countries’ legislation without any indication of which laws of these countries or which sections have been used in the analysis and development

b) While the Toolkit indicated in some places in the matrix to which laws have been used in the analysis, some of these laws are inappropriate or irrelevant to address the offences that they were intended to address. For instance, illegal interception is criminalised in Australia under the Telecommunications (Interception and Access) Act 1979 (Cth) not in Cybercrime Act 2001, Section 478.1, as the Toolkit mentioned. Another example also from Australia, the Toolkit noted that system interference is criminalised in Australia under Cybercrime Act 2001, Section 478.2, however, this Section intends to address illegal data interference not system interference. In fact, Sections 477.3 and 474.14 have provisions of illegal system interference. This, in fact, was illustrated in 2006 when the
AHTCC [236] reported that a person had been charged with ‘botnet’ and Distributed DoS attacks-related activities under Section 474.14 of the Criminal Code Act 1995 (Cth).

c) The ITU was developed by the American Bar Association’s Privacy & Computer Crime Committee and is not yet widely used. Schjolberg and Ghernaouti-Hélie (2009) [237] noted that “many countries preferred only making use of the Convention [CoE Convention] as a reference, and nothing more [including the ITU]”.

In 2009, Schjolberg and Ghernaouti-Hélie [237] noted that the CoE Convention was developed based on criminal conduct in the late 1990s and did not cover new criminal conducts, such as phishing, botnets and identity theft. Therefore, according to the authors, many countries are redeveloping new criminal provisions to make illegal the new types of malicious acts. The authors indicated that “[c]rimes against peace and security in cyberspace should be established as crimes under international law through a Convention or Protocol at the United Nations level”. The difficulty with this proposition is the time it takes to negotiate a global international convention. Indeed, quite recently, in April 2010, a proposal for a global cybercrime treaty has been rejected at the UN [63]. There are several reasons behind this rejection including the EU and USA view that there is no need for a new treaty since the CoE Convention exists [63].

At present, the CoE Convention is considered the major international development that intends to unify on an international basis criminal and procedural laws regarding computer-related crime [238]. Many jurisdictions are reforming their cybercrime legislation to bring them into line with the CoE Convention and, consequently, it is natural to advocate the role of the CoE Convention in developing a globally accepted convention on cybercrime. Schjolberg (2008) [239] recommended that “cybercrime legislation should be designed using existing international and regional frameworks as a reference or a guideline”. Therefore, it is important to consider the CoE Convention as a reference in any proposed new developments in computer crime or cybercrime legislation. Additionally, there are other reasons that contribute to the consideration of the CoE Convention including:
It is the major international development that aims to harmonise international laws concerning computer-related crime (although the ITU work in this area, as noted above, is also significant and needs to be considered).

There are many European countries such as the UK and other non-European countries such as the USA that have signed the CoE Convention [240, 241].

Because there are many countries that agreed to the CoE Convention, it is always easy to build upon and update its articles in order to accommodate other countries’ needs.

Schjolberg (2008) [239] indicates in his paper ‘The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva’ that:

_In order to reach a global harmonization of cybercrime legislation, and a common understanding of cybersecurity and cybercrime among countries at all stages of economic development, a global agreement or Protocol at the United Nations level should be established that includes solutions aimed at addressing the global challenges._

It seems very clear therefore 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 FATF regional bodies have cooperated successfully with the international FATF to achieve AML/CFT aims), a point we come back to further below:

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/)

Steps 1, 2 and 3 are addressed in more detail as follows.

**Step 1 – Identify the main players (international organisations)**

Computer crime or cybercrime is a global problem, and therefore it requires a global solution. Consequently, the main responsibility for solving global problems should be taken by a global organisation [241], the UN. Additionally, for their recognised efforts at the international level, the G8 and Interpol should have some input into the development of harmonised cybercrime legislation. Besides that, the work done by the CoE is very well known and recognised, and therefore, many countries have implemented some of the CoE Convention articles. At present, Kirk (2010) mentioned that 27 countries have ratified the CoE Convention along with more than 100 countries are using it as a basis for developing their cybercrime legislation [240]. For that, the CoE Convention could be very helpful in the area of combating computer crime and promoting harmonised legislation to combat such crimes. Harley (2010) noted that while there is a need for a global convention on cybercrime, it is inefficient to ignore the existing CoE Convention [241].

**Step 2 – Identify the sub-players (regional bodies)**

It is evident that multilateral or bilateral agreements are easier to accomplish than world-wide agreements when it comes to developing harmonization of any sort. Therefore, dividing the countries based on their regions and relation to each other will arguably speed up the process of harmonising cybercrime legislation. Currently, the FATF Style Regional Bodies exist and therefore, it would be arguably possible in principle to involve such regional bodies or similar organisations in the development of harmonised cybercrime legislation.

The development of international standards for combating money laundering and financing of terrorism (AML/CFT) under the aegis of the FATF exemplifies the
importance of regional participation in achieving international consensus. While the FATF was established in 1989 by the G7 in response to increased concern about money laundering, its standards have been accepted by the UN, the International Monetary Fund (IMF) and the World Bank. In fact, there are 35 members of the FATF which include 33 countries (from all the five continents) and 2 regional organizations (European Commission and Gulf Co-operation Council (GCC)) Most relevant is the fact that the FATF is also working closely with the following FATF Style Regional Bodies (associated members) [172]:

- Asia/Pacific Group on Money Laundering (APG)
- Caribbean Financial Action Task Force (CFATF)
- Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)
- Financial Action Task Force on Money Laundering in South America (GAFISUD)
- Middle East and North Africa Financial Action Task Force (MENAFATF)
- Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- Intergovernmental Action Group against Money-Laundering in Africa (GIABA).

The work done by the FATF and the FATF Style Regional Bodies in cooperation to facilitate similar or comparable approaches for implementing AML/CFT system suggests a similar approach in achieving harmonized cybercrime legislation internationally. While the FATF recommendations are not fully implemented by some member countries, these recommendations are still considered as an important framework for countries to use in order to counter money laundering and terrorist financing. The focus here is to observe the advantages that the FATF experience creates for implementing a harmonised AML/CFT system and how it succeeded in bringing these different countries and organisations to agree on international standards for AML/CFT systems.

**Step 3 – Identify relationships**

The UN and the related regional bodies must identify their relationships, how they communicate and how they operate. Indeed, the proposed strategy will require
initiating national and international networks between private and public organisations. Broadhurst (2006) [221] indicates that combating computer crime requires “a variety of new networks: networks between police and other agencies within government, networks between police and private institutions, and networks of police across national borders”.

Regional bodies play important roles in their regions and should identify the extent to which the UN Convention on Cybercrime could be implemented and developed within their regions. The regional bodies should assess the member countries and also understand and identify their region-specific requirements. For instance, a particular article or law could be implemented in one region or country and may not be implemented elsewhere, yet the development of a legal system in a country could reflect its culture and other local factors. In fact, the computer crime or cybercrime legislation enacted in the UAE has some articles that reflect its specific culture and such considerations must be taken into account in the process and this is best done initially at the regional level. Thereafter, the UN must then consider each region’s requirements when assessing the member countries alignment with its articles and prioritise the implementation of its articles.

An Example

The UAE’s culture has developed from a strong belief in Islam, which is a way of life and governs the people’s behaviours and decisions [117]. Islam had a significant impact on the UAE culture and accordingly, the UAE culture has evolved differently from the cultures in Australia, the UK and the USA. Cultural factors affect how a country develops its legal systems. The UAE society is conservative when it comes to what they believe. Some types of Articles under the UAE Federal Law No (2) of 2006 clearly support this argument. Article 12 relates to sexual exploitation and makes illegal the use of the Internet or any high-tech device for producing, preparing, sending or saving with the intent to exploit, distribute or provide others with material that can harm public safety and encourage sexual exploitation. Additionally, Article 13 makes illegal the use of the Internet or any high-tech device for encouraging males or females to commit adultery or prostitution or help them to do so. The influence of religious factors on Article 15 of the UAE Law is most obvious. Article 15 criminalises the use of the Internet or
high-tech device for abusing any Islamic holy shrines or rituals, abusing the shrines or rituals of other religions, insulting a recognized religion, or stimulating or promoting sins.

Article 16 makes illegal the use of the Internet or high-tech devices for transcending family principles or values, or publishing news or pictures concerning private lives and the family. The second part of Article 16 could result in some controversial cases, because of the increasing power the UK and the USA give the media more freedom; this is particularly obvious when they cover the news and private lives of celebrities. Kierkegaard (2007) [242] notes that “Asia is characterised by a cultural diversity that allows societies to adopt practices unique to their value systems and historical experience”. Kierkegaard indicates that what may be considered a harmful or criminal act in one jurisdiction, may be considered acceptable in another jurisdiction.

3.3.2 Summary
Similar to the FATF experience, the UN and appropriate regional bodies should work together to bridge the gap between different computer crime and cybercrime legislation around the world. Additionally, the UN should establish assessment criteria to evaluate each country’s legislation. The regional bodies are responsible for evaluating their members and provide reports and feedback to the UN.

3.4 Conclusion
We have proposed a new and more comprehensive cybercrime taxonomy that refines and extends previous taxonomies. Our taxonomy is based on both the role of the computer in a crime and also on some significant contextual markers of a crime. We believe this detailed taxonomy covers all computer-related crimes and meets the needs of law enforcement agencies and the international community when identifying, reporting, monitoring and addressing computer crime. Additionally, we have proposed a consistent codification of computer crime that builds upon our proposed taxonomy.
Our analysis has shown that Australia, the UAE, the UK and the USA have all adopted legislation that covers all the CoE Convention Articles 2 to 11. However, not all of the computer offences are criminalised under the one legislation, but rather under different legislations. Overall, the findings show the existence of legislation in Australia, the UAE, the UK and the USA that corresponds to Articles 2 to 11 of the CoE Convention with one exception: the UAE legislation does not have provisions corresponding to Article 6 of the CoE Convention. All four countries have provisions for the punishment of committing a computer-related offence. Additionally, we have investigated the extent to which there is alignment of the legislation enacted in Australia, the UAE, the UK and the USA with the Articles 2 to 11 of the Convention. The results of this preliminary analysis indicate that the degree of alignment with Articles 2 to 11 of the CoE Convention is low in Australia and the UK and very low in the UAE. We believe a regional approach as we describe in Section 3.3 is required to progress activities on this front. The UAE legislation is also required to be updated to cover some important conditions of the CoE Convention.

Computer crime or cybercrime is a global problem which requires harmonised laws and global cooperation to be combated effectively and there are problems concerning such laws on the global scale. Recent rejection by the UN of a proposal for an international cybercrime treaty highlights the point. The need for harmonised cybercrime legislation is a need that will not go away and this chapter has presented a proposal for a new strategy for developing harmonised cybercrime legislation globally.

The next chapter examines the ADP (Abu Dhabi Police, UAE) and QPS (Queensland Police Service, Australia) approaches for combating computer-related crime.
Chapter 4
Case Study: Combating Computer Crime in Australia and the UAE

Chapter 3 proposed a refined and extended taxonomy of computer crime that identifies how computer crimes may be classified based upon the dual characteristics of the role of the computer and the contextual nature of the crime. It also presented a comparative review of the cybercrime legislations enacted in Australia, the UAE, the UK and the USA and how that corresponds to the CoE Convention on Cybercrime and proposed a new framework to develop harmonised computer crime or cybercrime legislation globally.

This chapter identifies, examines and compares 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. Identifying the law enforcement procedures employed has in each case focused on the responsible law enforcement agency, the Queensland Police Force (QPS) and the Abu Dhabi Police (ADP) respectively. In order to achieve the objectives, we were given access by the respective law enforcement agencies to some relevant departmental sections. Because we could not find documented procedures on how computer crime units in both QPS and ADP investigate computer crime, identifying the procedures has been achieved through the use of questionnaires completed by the officers and by face to face interviews. A benefit of this approach has been 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. As indicated in Chapter 2, each law enforcement agency was analysed separately first using within-case
analysis, then we compared the results for both agencies using cross-case analysis. Analysis of the resulting data indicates how the procedures and approaches to combat computer crime by these two law enforcement agencies compare and the implications for improvements to achieve better approaches for combating computer crime in these two jurisdictions and, by extension, internationally.

Overall, chapter 4 addresses the following research question:

**Q2. To what extent are the approaches for combating computer crime in Australia (as represented by the QPS) and the UAE (as represented by the ADP) different and what improvements are needed?**

Section 4.1 below describes our approach in more detail how the data was gathered and analysed. Section 4.2 then summarises and analyses in detail the responses across the two agencies, the QPS and the ADP. Finally, Section 4.3 discusses the findings and based on that identifies improvements that are needed and challenges to be faced by each agency and the implications generally for the international community.

Some of the results presented in this chapter have been published in the following conference paper:


**4.1 Methodology**

This section discusses how the Phase I and Phase II data collections were conducted for each of the two law enforcement agencies, Queensland Police Service (QPS) and Abu Dhabi Police (ADP). Our data collection was conducted in two phases, Phase I and Phase II. Each phase consisted of developing a questionnaire and collating responses to it, followed by face to face interviews to clarify or elaborate upon those responses. At the end of each phase, the data gathered was consolidated and analysed.

---

9 We note that we have omitted detailed information regarding or provided by the interviewees which might compromise their anonymity.
4.1 Methodology

The Phase I and Phase II questionnaires and interview questions appear in the following Appendices:

- Appendix C: Questionnaires and interview questions – Phase I
- Appendix D: Questionnaires and interview questions – Phase II

4.1.1 Overall Methodology

While the purpose of Chapter 4 is to answer the second research question, this question is further refined in terms of the following three propositions:

**Proposition 1**: The legislation used in Queensland to counter computer crime is different to that used in Abu Dhabi.

**Proposition 2**: The policy, procedures, technology and staff resources used in Queensland to counter computer crime are different to those used in Abu Dhabi.

**Proposition 3**: The nature and extent of computer crime or cybercrime in Queensland is different to that in Abu Dhabi.

The intention in testing these propositions is to identify similarities and differences between the approaches used by the two agencies, and most importantly, to identify the challenges they face and the improvements that are needed.

**Unit selection**

The focus within the two agencies is on specific police units which are particularly responsible for combating computer crime. In relation to the ADP, the focus is on the Computer Crime Unit (CCU) and in terms of the QPS, on the four police units: Computer Crime Investigation Unit (CCIU), Identity Crime Unit (IDCU), Proceeds of Crime Unit (PoCU), and Forensic Computer Examination Unit (FCEU). The four QPS units involved in this particular area of criminal investigation operate under the Fraud and Corporate Crime Group/State Crime Operations Command.

**Questionnaire development**

The propositions listed above guided the creation of the questionnaires and interview questions. The 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.

The Phase I written questionnaire was developed based on our literature review and on prior informal discussion with the QPS. For the QPS questionnaire, there were 15 general questions and 4 (for CCIU and IDCU) or 5 (for PoCU and FCEU) specific questions related to each unit under study. For the ADP questionnaire, there were 15 general questions and 4, 4, 5 and 5 questions related to computer crime, identity theft, money laundering, and computer forensics, respectively. Then, after analysing the questionnaires responses, we developed the follow-up interview questions. The number of interview questions varied from one participant to another as these interview questions were based on each individual’s responses to the questionnaires questions.

Analysis of Phase I found that responses in some areas required further clarification due to issues of obviously incorrect responses and inconsistent responses. Besides that, and most importantly, given the fact that Phase I was a pilot study, Phase I highlighted that there was a need to address several additional areas and questions.

The additional areas were:

• the nature of the legislation used regarding search warrants/seizure and data interception and the procedures followed
• the nature of the different stages of the process of investigating and prosecuting a computer crime (complaint, report, initial referral, initial investigation, substantial possibly multi-party investigation, final report, and prosecution)
• problems in coping with computer crime legislation that differs between countries

The additional questions were:

• Are there policy and procedures documents in the QPS and the ADP, if so how are they made known?
• How does the computer crime unit within ADP cooperate with other sections or units within ADP during a computer crime investigation?
• Given the ADP does not have a computer forensic laboratory or section, how can it then seize and/or analyse computers or high-tech hardware or files?
• Regarding the computer crimes investigated by QPS and ADP, do they have statistics about actual numbers of: cases investigated? Solved? Unsolved? Prosecuted?
• How can the investigators prioritise which crime comes first when there are no guidelines available?
• If there were reasons to create a computer-related crime database, how can computer crime be classified? And based on what?
• What is the possibility of getting the QPS or ADP existing guidelines even if still under development?
• What is the extent of computer crime in Queensland and Abu Dhabi?

The Phase II questionnaires were developed based on the areas and questions listed above. While Phase I questionnaires were the same for both QPS and ADP, different Phase II questionnaires were developed for the two agencies. For QPS, the questions were structured according to each unit. In fact, there were 16, 15, 10 and 5 questions developed for CCIU, IDCU, PoCU and FCEU, respectively. With regards to the ADP, there were 23 questions developed and structured to be answered by the ADP participants. Additionally, the number of interview questions varied from person to person and these depended mainly on each participant’s responses to the questionnaire questions.

4.1.2 Phase I – Pilot Study

Phase I was conducted in 2007. The data was first gathered from the ADP and then from QPS. It was compiled and analysed from the 15th of November 2007 until the 24th of January 2008. The full questionnaires and interview questions of Phase I are attached in Appendix C.
4.1 Methodology

**ADP – Computer Crime Unit (CCU)**

Phase I was conducted in Abu Dhabi in June 2007. The written questionnaires were distributed on the 10th of June 2007 and completed on the 14th of June 2007. The interviews were done on the 11th and 12th of June 2007.

**QPS – Computer Crime Investigation Unit (CCIU), Identity Crime Unit (IDCU), Proceeds of Crime Unit (PoCU), Forensic Computer Examination Unit (FCEU)**

Phase I was conducted in Brisbane within the period from May to November 2007. The written questionnaires were distributed on the 14th of May 2007 and completed on the 27th of October 2007. The interviews were started on the 30th of October and completed on the 13th of November 2007.

### 4.1.3 Phase II – Further Study

The second phase was conducted in 2008 and included performing follow-up in-depth studies using written questionnaires and interviews in cooperation with QPS and ADP. This time, and as outlined above, new written questionnaires were developed based on the results of Phase I outlined earlier. The complete questionnaires and interview questions of Phase II are attached in Appendix D.

**ADP – Computer Crime Unit (CCU)**

The study was conducted in the period from March to May 2008. The written questionnaires were completed on the 18th of March 2008. The interviews were done in the period from the 7th to the 16th of May 2008. The purpose of Phase II was to clarify issues that had arisen from Phase I.

**QPS – Computer Crime Investigation Unit (CCIU), Identity Crime Unit (IDCU), Proceeds of Crime Unit (PoCU), Forensic Computer Examination Unit (FCEU)**

The study was conducted within the period from February to September 2008. The written questionnaires were distributed on the 25th of February 2008 and completed on the 3rd of June 2008. The interviews were started on the 4th of July and completed on the 10th of September 2008. The aim was to clarify the issues that had arisen in the Phase I.
4.2 Cross-Case Findings – QPS vs. ADP

This section presents the results of the detailed cross-comparison of the procedures and approaches used by QPS (Queensland) and ADP (Abu Dhabi) for combating computer crime. It aims to answer the second research question (Q2) and addresses the three propositions mentioned in Sub-section 4.1.1. The intention in testing these propositions is to identify improvements that may be needed in order to improve the approaches used for combating computer crime. These three propositions and the comparison of the related results from the QPS and the ADP are discussed within the next sub-sections.

The results presented and discussed in this section are based upon the analysis of the Phase I and II questionnaires responses and face to face interviews. All the related information regarding the Phase I and Phase II questionnaires and interview questions appear in the following Appendices:

- Appendix C: Questionnaires and interview questions – Phase I
- Appendix D: Questionnaires and interview questions – Phase II

4.2.1 Proposition 1 – Legislation and Jurisdiction

The first proposition is about comparing the QPS (Queensland) with the ADP (Abu Dhabi) within the theme of legislation and jurisdiction:

**Proposition 1:** The legislation used in Queensland to counter computer crime is different to that used in Abu Dhabi.

Table 4.1 is a matrix of the comparison resulting from the analysis of the responses from QPS and ADP regarding the first theme, legislation and jurisdiction. From Table 4.1, there are some similarities and differences between the two jurisdictions. One major difference is that the QPS follows the state and federal legislations, the ADP uses only the federal legislation.

Noteworthy is that the UAE Federal Law No 2 of 2006 covers a wide range of offences and that it might be an advantage for the ADP investigators. However, this is not the same case with the QPS investigators. In fact, they use several federal and state legislations to prosecute computer crime. For instance, unlike the UAE Federal Law which criminalises money laundering, money laundering is not
criminalised under the Queensland computer crime legislation but under the Criminal Proceeds Confiscation Act 2002 (Queensland).

Table 4.1
Cross case comparison for the first proposition

<table>
<thead>
<tr>
<th>The area of comparison</th>
<th>QPS (Queensland)</th>
<th>ADP (Abu Dhabi)</th>
</tr>
</thead>
<tbody>
<tr>
<td>There exists state legislation which covers cybercrime</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>There exists federal legislation which covers cybercrime</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>The law enforcement agency has jurisdiction over cases wholly or partially happening in the state</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Awareness of how to deal with multi-jurisdiction computer crime cases</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Awareness of what to do when the alleged offence is located overseas</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

As regards jurisdiction, we have found that ADP participants identify the location of the offence based on the location of the victim; this means that the state, where the victim’s computer is located, is responsible for the investigation. On the other hand, the QPS participants indicated that the state, where the offender is located, is responsible for the investigation.

In Chapter 3, we compared the computer crime and cybercrime legislation used in Australia, the UAE, the UK and the USA, and how they correspond to the criminal provisions provided by the CoE Convention. We found that Australia and the UAE have legislation that covers the offences identified under Articles 2 to 11 of the CoE Convention, except that the UAE legislation does not have provisions on Article 6 of the CoE Convention concerning misuse of devices. However, not all of these offences are criminalised, in Australia and the UAE, under one legislation, but are covered under different legislation. In contrast to the UAE, committing one of the computer-related offences in Australia is more likely to be punished with only an imprisonment term. Additionally, the UAE criminal sanctions system has smaller and lighter punishments compared to the other countries.

4.2.2 Proposition 2 – Policy, Procedures and Resources

The second proposition relates to comparing the themes of the policy, procedures and technology used by the QPS (Queensland) and the ADP (Abu Dhabi):
**Proposition 2:** The policy, procedures, technology and staff resources used in Queensland to counter computer crime are different to those used in Abu Dhabi.

Testing the above proposition was done by comparing QPS with ADP using the following themes to identify the similarities and differences:

- Policy and procedures
- Investigation processes
- Officer Experience
- Resources – Technology and computer forensics resources
- Time to investigate computer crime
- Education and training
- Reporting and statistics.

**Policy and procedures**

A standard operating procedure (SOP) is a document that specifies the procedures that should be followed in order to complete an activity [243]\(^\text{10}\). The ADP participants noted that the policy and SOP documents are still under development. Thought, some of the QPS participants mentioned that they have SOP documents in relation to investigating identity theft and proceeds of crime, other participants from the CCIU indicated that their SOP document is still under development. Overall, the responses from both QPS and ADP indicated that their SOP documents concerning the investigation of computer-related crime are still under development, with the exception of some documented procedures relating to search and seizure.

The QPS and ADP receive the complaints from similar sources:

\(^{10}\) According to the USA Environmental Protection Agency (EPA), a standard operation procedure (SOP) is:

> a set of written instructions that document a routine or repetitive activity followed by an organization. The development and use of SOPs are an integral part of a successful quality system as it provides individuals with the information to perform a job properly, and facilitates consistency in the quality and integrity of a product or end-result ... The development and use of SOPs minimizes variation and promotes quality through consistent implementation of a process or procedure within the organization, even if there are temporary or permanent personnel changes.
Chapter 4: Case Study: Combating Computer Crime in Australia and the UAE

- QPS: Police stations, the public, other state’s police, government agencies
- ADP: Police stations, the public, other emirate’s (state) police, government agencies.

Some participants from both QPS and ADP noted that the investigation is in some cases carried out by more than one unit or section, each with its own responsibility. This means in some cases the investigation will be carried out by the computer crime unit in QPS or ADP along with other units within the same police force related to the case. However, the main responsibility would be carried out by computer crime units if the case is computer-related, otherwise, by another unit or section of the police. For instance, identity crime would be investigated by the IDCU of QPS and CCIU, and the IDCU will take the main responsibility for the investigation.

With regard to requesting the authorisation of search warrants and court orders prior to conducting the search, seizure, and interception of communications:

- QPS participants indicated that the investigating officer (case officer) prepares and requests the authorisation for warrants and court orders
- ADP participants indicated that the head of CCU requests such warrants.

The majority of QPS and ADP participants noted that most of the cases that have been investigated in the last 12 months required warrants and court orders. These participants mentioned that they have procedure documents that identify what and how tasks should be carried out during the investigation for the search and seizure. QPS participants indicated that their procedure documents are available both as a hard copy and online document. Nevertheless, these procedure documents are related only to specific circumstances about the search and seizure. Neither QPS nor ADP have SOP documents for investigation of computer crime, according to the majority of the participants working in the computer crime units.

**Investigation processes**

The ADP indicated that their investigation processes consisted of 15 stages, and these are listed in Table 4.2. The QPS indicated that their investigation processes consisted of 12 stages, and these are listed in Table 4.3.
Table 4.2
The ADP investigation processes

<table>
<thead>
<tr>
<th>Stage #</th>
<th>Stage detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The complainant reports the offence</td>
</tr>
<tr>
<td>2</td>
<td>The available information is analysed</td>
</tr>
<tr>
<td>3</td>
<td>The police station where the offence is reported sends the report to the CCU</td>
</tr>
<tr>
<td>4</td>
<td>The investigation is commenced</td>
</tr>
<tr>
<td>5</td>
<td>The suspect’s location based on the IP address is identified</td>
</tr>
<tr>
<td>6</td>
<td>The ISP is contacted to identify the suspect’s location</td>
</tr>
<tr>
<td>7</td>
<td>The suspect is interviewed</td>
</tr>
<tr>
<td>8</td>
<td>Search warrants for conducting the search and seizure are requested</td>
</tr>
<tr>
<td>9</td>
<td>The search and seizure is executed</td>
</tr>
<tr>
<td>10</td>
<td>Seized evidence and devices sent to the Public Prosecutions</td>
</tr>
<tr>
<td>11</td>
<td>The Public Prosecutions give the order for examining the devices</td>
</tr>
<tr>
<td>12</td>
<td>Evidence gathered from the devices</td>
</tr>
<tr>
<td>13</td>
<td>The results sent to the Public Prosecutions</td>
</tr>
<tr>
<td>14</td>
<td>The Public Prosecutions examines all available evidence</td>
</tr>
<tr>
<td>15</td>
<td>Evidence submitted to the court</td>
</tr>
</tbody>
</table>

Table 4.3
The QPS investigation processes

<table>
<thead>
<tr>
<th>Stage #</th>
<th>Stage detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The complainant reports the offence</td>
</tr>
<tr>
<td>2</td>
<td>A criminal act that has been committed is assessed</td>
</tr>
<tr>
<td>3</td>
<td>The jurisdiction is assessed</td>
</tr>
<tr>
<td>4</td>
<td>Information from the complainant is obtained</td>
</tr>
<tr>
<td>5</td>
<td>Evidence is reviewed</td>
</tr>
<tr>
<td>6</td>
<td>The relevant legislation is assessed</td>
</tr>
<tr>
<td>7</td>
<td>The allegation is investigated</td>
</tr>
<tr>
<td>8</td>
<td>Legislation against the evidence is reviewed</td>
</tr>
<tr>
<td>9</td>
<td>All procedures that have been followed are confirmed</td>
</tr>
<tr>
<td>10</td>
<td>Search warrants are executed</td>
</tr>
<tr>
<td>11</td>
<td>Suspects are interviewed in order to determine two factors: (a) sufficiency of evidence, and (b) public interest test</td>
</tr>
<tr>
<td>12</td>
<td>Suspects are prosecuted or the case is closed</td>
</tr>
</tbody>
</table>

Based on the literature ([127], [128], [130], [136], [137], [18], [244] and [107]), investigating a computer crime includes the following five stages (processes):

- Complaint or initial report of the alleged offence
- Initial investigation
- Substantial (possibly multi party or joint) investigation
- Prosecution
- Final reporting.

Responses from QPS and ADP participants indicate how the stages they had identified mapped to the above stages, this mapping is provided in Table 4.4.

Generally, the QPS and ADP investigation stages are very similar. Also, we can observe from Tables 4.2 and 4.3 that some of the ADP investigation stages appear only in one of the QPS investigation stages. For instance, stages 8, 9 and 10 of the ADP investigation are comparable to stage 10 of the QPS investigation. Overall, both the QPS and ADP investigation processes are related to the five investigation stages in Table 4.4.

Table 4.4
Identify how the investigation process of ADP and QPS related to the five investigation stages

<table>
<thead>
<tr>
<th>#</th>
<th>Stage or process detail</th>
<th>Investigation stages (ADP)</th>
<th>Investigation stages (QPS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Complaint or initial report of the alleged offence</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Initial investigation</td>
<td>2, 3, 4, 5, 6</td>
<td>2, 3, 4, 5, 6</td>
</tr>
<tr>
<td>3</td>
<td>Substantial (possibly multi party or joint) investigation</td>
<td>7, 8, 9, 10, 11, 12, 13</td>
<td>7, 8, 9, 10, 11</td>
</tr>
<tr>
<td>4</td>
<td>Prosecution</td>
<td>14</td>
<td>12</td>
</tr>
<tr>
<td>5</td>
<td>Final reporting</td>
<td>15</td>
<td>12</td>
</tr>
</tbody>
</table>

**Officer Experience**

The range of experience in the police force for QPS participants is from 12 to 25 years, and for ADP from 7 to 18 years. Also, the range of experience in dealing with computer crime is from eight months to a maximum of eight years for QPS participants and from six months to a maximum of three years for ADP participants. In conclusion, generally, the QPS participants are more experienced in the police force and in their units than the APD participants. This may be more a reflection of the fact that the UAE issued its first computer crime legislation as recently as 2006.
**Resources - Technology and computer forensics resources**

Computer forensics is a science and requires special skills, software, and tools to be effective in discovering and analysing the electronic evidence. Mohay et al. (2003) [59] indicate that computer forensics intends to identify, preserve, analyse, and present to a court of law evidence which derives from a digital (computer) source and that the relevant technology and tools can be classified in three major categories:

- secure
- analyse
- present.

Analysis of responses regarding computer forensics resources in both QPS and ADP shows that while the QPS has a unit which specializes in computer forensic examinations, the ADP does not have a special computer forensic unit. This, in fact, is a big gap between the two cases of study.

In relation to the above three categories, the QPS investigators secure the evidence using a number of write blocker hardware (e.g., Tableau T35i) and software (e.g., X-Ways forensic software) to allow the acquisition of information on a digital device without altering or damaging the device's contents. Additionally, the FCEU of the QPS uses a number of tools for conducting digital forensic analysis such as Forensic Toolkit (FTK) and X-ways Forensics. The third category regarding the presentation of evidence starts after the investigators secure and analyse the electronic evidence. It requires the investigators to present the secured and analysed evidence in a way which is readable and understandable in the court.

**Time to investigate computer crime**

Generally speaking about ADP and QPS, the investigation starts within 24 hours from receiving the complaint. According to the ADP participants, the investigation takes around one week to be completed. However, this is a questionable time period since some computer crimes are very complicated to investigate and may involve multi-jurisdiction law enforcement agencies. In contrast, and according to some QPS participants, there is no average time for how long the investigation
takes to be finalized. Other QPS participants indicated the average is around 28
days to one month. However, the QPS participants’ responses vary and this may be
a reflection of the fact that these participants are working under four different
units.

**Education and training**

The responses indicated that the QPS and ADP use a number of training courses to
upgrade the investigators’ skills, as illustrated in Table 4.5. Because the ADP
participants did not mention the type of training courses the ADP used, as a result,
two of the training courses may be IT and investigative courses, but this was not
confirmed in Table 4.5.

<table>
<thead>
<tr>
<th>Type of courses or programs used to upgrade the skills of the investigators</th>
<th>Used by QPS</th>
<th>Used by ADP</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT courses</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Investigative courses</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Training courses</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>In-house training</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Personal Research</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Job experience</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Attending Conferences and seminars</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Visiting developed countries</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Though there are no specific forensic or IT requirements to employ personnel
in the CCIU in QPS, individuals with IT backgrounds are preferred. In contrast, the
CCU in ADP requires a specific educational level to employ its personnel such as a
Diploma in IT and specialist courses in computer networks. Additionally, both QPS
and ADP participants noted that their units have a role in educating the public
about computer crimes such as identity theft, online fraud, malicious code,
Phishing and credit card fraud.

**Reporting and statistics**

QPS reports the outcome of an investigation to:
• D/Supt of the Fraud and Corporate Crime Group
• The Crime and Misconduct Commission (CMC)
• The Office of the Director of Public Prosecutions (DPP)
• Other sections of QPS
• The investigator making request
• The source of the complaint
• The court
• Qprime (the crime reporting database).

ADP only reports the outcome of the investigation officially to the public prosecutor. The public prosecutor will then investigate the evidence which may require further investigation or reject the evidence before submitting it to the court. The ADP participants refer to submitting the final outcome report only to the public prosecutor, although other agencies may be notified of the final outcome of the investigation. Nevertheless, the QPS and ADP generally report the outcome of the investigation in different types as shown in Table 4.6.

Table 4.6
Type of outcome reports used by QPS and ADP

<table>
<thead>
<tr>
<th>Type of the outcome report</th>
<th>Used by QPS</th>
<th>Used by ADP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verbally</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Written report</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Letter</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Fax</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Email</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Specific forms</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

4.2.3 Proposition 3 – Nature and Extent of Computer Crime

The third proposition is about comparing the nature and extent of computer crime in QPS (Queensland) with that in ADP (Abu Dhabi):

Proposition 3: The nature and extent of computer crime or cybercrime in Queensland is different to that in Abu Dhabi.
With regard to the nature and extent of computer crime category, we compared between ADP (Abu Dhabi) and QPS (Queensland) according to three aspects:

- the type of computer offences investigated;
- the availability of a comprehensive database about computer crime that has occurred; and
- priorities when investigating computer crime.

In the experience of the officers interviewed, Table 4.7 illustrates the type of computer crime that has occurred and investigated by both of ADP and QPS. The following computer crimes were reported by QPS but not by ADP participants:

- Malicious code
- Theft of service
- Denial of service (DoS) attacks
- Online auction fraud
- Scams
- Cyber stalking
- Intellectual property
- Social engineering fraud.

The second point of comparison is comparing the existence of a comprehensive database for computer crime. Both QPS and ADP do not have a specific database for computer-related crimes. The offences occurring in Queensland are recorded in the Queensland crime reporting database. Nothing is mentioned regarding the keeping of electronic records in database about offences occurring in Abu Dhabi.

The last aspect regarding this proposition was regarding the priority of the crime. It is clear that there are no guidelines and procedures to prioritise the investigation of the type of computer crime in both QPS and ADP. However, the investigator has the responsibility to prioritise based on the categories of crime. Because there are no guidelines to prioritise the type of computer crimes that should be investigated firstly, the investigator has to decide which crime is more serious and should be investigated first. Crimes that have an impact on the government sectors or public safety are always on a high priority. For instance,
crimes that affect national security have high priority and usually such crimes are referred to the federal police in both countries for the investigation.

Table 4.7
Type of computer crime investigated by QPS and ADP participants

<table>
<thead>
<tr>
<th>The type of crime investigated by the agency</th>
<th>QPS (Queensland)</th>
<th>ADP (Abu Dhabi)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access (hacking, cracking)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Malicious code</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Theft of service</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Denial of service (DoS) attacks</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Credit card fraud</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Online auction fraud</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Online banking fraud</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Child pornography</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Scams</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Cyber stalking</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Intellectual property</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Copyright crimes</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Harassment</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Social engineering fraud</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Online identity theft</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Online money laundering</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Phishing</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Electronic manipulation of sharemarkets</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Forgery</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Furthermore, the QPS and ADP participants have provided statistics concerning computer crime for the 12 month period commencing from the date of the Phase II questionnaire (March 2008 for ADP, April 2008 for QPS). Their responses are presented in Table 4.8.

Overall, from Table 4.8, we can see in general that the number of crimes reported to be investigated in Queensland is more than the number of crimes reported to be investigated in Abu Dhabi. We assume that one factor may be the population of each place - Abu Dhabi has a smaller population compared to Queensland. According to the Abu Dhabi Government (2010) [245], the Abu Dhabi population was estimated around 1.5 million in mid 2008. The Queensland population at June 2008 was estimated around 4.29 million (Australian Bureau of Statistics 2009) [246].
Table 4.8
Type of crime and number of cases investigated by QPS and ADP participants over 12 months from the date of the Phase II questionnaire (March 2008 for ADP, April 2008 for QPS)

<table>
<thead>
<tr>
<th>Type of crime</th>
<th>Number of cases investigated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access</td>
<td>ADP 4, QPS 2</td>
</tr>
<tr>
<td>Malicious code</td>
<td>ADP 0, QPS 0</td>
</tr>
<tr>
<td>Denial of service (DoS) attacks</td>
<td>ADP 0, QPS 0</td>
</tr>
<tr>
<td>Online fraud</td>
<td>ADP 3, QPS 28</td>
</tr>
<tr>
<td>Identity theft</td>
<td>ADP 1, QPS 2</td>
</tr>
<tr>
<td>Harassment</td>
<td>ADP 3, QPS 20</td>
</tr>
</tbody>
</table>

It is interesting to note that malicious code and DoS attacks have not been investigated by either ADP or QPS over 12 months from the date of the Phase II questionnaire (March 2008 for ADP, April 2008 for QPS). Yet, these statistics presented in Table 4.8 show the number of cases that were reported to have been investigated by QPS and ADP participants in the last 12 months since the time of Phase II questionnaire. Therefore, there is no indication of how many other cases which were not reported in Table 4.8 that were actually handed over to be investigated primarily by the federal police in both countries.

4.3 Discussion
This section summarises the main findings arising from our analysis of responses presented in Section 4.2 and discusses the extent to which Propositions 1, 2 and 3 are in fact verified. It also discusses the implications of this research regarding what improvements are needed in order to update the existing approaches for combating computer crime used by QPS and ADP. These implications in turn raise awareness of issues to be highlighted and prioritized by law enforcement agencies internationally.

4.3.1 Summary of Findings
Our analysis of the responses we have collated from the Phase I and II questionnaires and face to face interviews indicates that there are some differences between the approaches for combating computer crime in Queensland (Australia) and Abu Dhabi (UAE).
We found that the results of the study support largely the argument of the first and second propositions and partially support the argument of the third proposition. The following paragraphs summarise the results of the study in relation to these three propositions.

We found that there are some differences between the two jurisdictions regarding computer crime legislation and that the first proposition is largely supported albeit the differences are not huge. They arise due to the role of states in the case of Australia rather than in the UAE, and due to cultural and religious influences. We also found that while QPS participants indicated that the jurisdiction was determined by where the offender is located, the ADP participants identify jurisdiction based on the location of the victim. This means, in the case of Type I computer crimes, that the jurisdiction where the victim's computer is located is responsible for the investigation.

The analysis between QPS and ADP in terms of the themes of policy, procedures and technology has largely supported the argument of the second proposition. The responses show that both QPS and ADP do not have documented procedures for investigating computer crime. The responses also indicate that the QPS participants are more experienced in the police force and in their units than the APD participants. Also, in contrast to the QPS, the ADP does not have a special computer forensic laboratory. This is a considerable gap between the two police forces.

We found that the nature and extent of computer crime in both Queensland and Abu Dhabi have not unexpectedly some marked similarities, there are however some differences. Therefore, the results show that the third proposition is partially supported. The responses showed that some of the crimes occur in both Queensland and Abu Dhabi such as computer hacking, online fraud, identity theft, and online scams. However, some other crimes such as cyber stalking and harassment appear to have occurred in the one jurisdiction only. Additionally, neither QPS nor ADP has a specific database for computer crime. The QPS and ADP participants indicated that there are no guidelines and procedures to prioritise investigation of the type of computer crime. The case investigator has the
responsibility to prioritise such crime based on which crime is more serious and should be investigated first.

Our analysis of QPS and ADP responses, summarized above, has identified some important improvements that are needed, and challenges and issues that continue to create problems for the two law enforcement agencies such as insufficient resources, and coping with computer crime legislation that differs between countries (jurisdictional issues and cooperation between countries). We address these needed improvements and challenges below.

4.3.2 Needed Improvements and Challenges

The main purpose of this chapter is to compare the QPS and ADP approaches and to identify what improvements are needed. Therefore, this sub-section discusses the needed improvements and also the existing challenges and issues that pose a real problem for the computer crime investigators.

Our analysis of the responses has identified a number of areas where improvements are needed in order to update existing QPS and ADP approaches for combating computer 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. ADP needs to establish a unit that specializes in computer forensics examinations
4. reporting and recording of computer crimes as distinct from other forms of crime
5. setting plans to overcome the existing challenges and issues internally and also via cooperating with other law enforcement agencies to combat computer crime.

Based on the literature, we identified several issues and challenges in the questionnaire that may pose problems for law enforcement agencies such as the QPS and ADP. The QPS and ADP participants then noted the particular challenges and issues that were creating problems in their investigations. Some of the challenges and issues may be handled internally; but other challenges need to be
addressed externally in cooperation with other jurisdictions. The participants of QPS and ADP both noted that there are problems resulting from coping with computer crime legislation that differs between countries. They indicated that an offence in one jurisdiction may not be an offence in another jurisdiction because some countries are still upgrading their legislation to cover computer-related crime. QPS has established partnerships with national and international agencies and business organizations (e.g., Microsoft) in order to overcome some of the jurisdictional and cooperation problems.

In order to identify additional areas where improvements are needed, the second questionnaire focused more on the following important challenges and issues:

- Training and resources
- Updating expertise
- Cooperation with other organization or law enforcement
- Jurisdictional problems of computer crime
- Anonymity services
- Coping with computer crime legislation that differs between countries.

Table 4.9 illustrates how QPS and ADP approach the key challenges and issues. Table 4.9 shows that the QPS participants do have more initiatives and activities to manage the identified challenges and issues.

### 4.4 Conclusion

This chapter reports on the analysis of procedures and practices of combating computer crime used by ADP from the UAE, and QPS from Australia. The analysis answered the three propositions related to the second research question and indicates that there are some differences between the approaches for combating computer crime in Queensland (Australia) and Abu Dhabi (UAE). We have found that while QPS has a unit which specializes in computer forensic examinations, ADP does not have a special computer forensic laboratory. This is a significant difference. Also, the study found that neither QPS nor ADP have a specific database for computer crime and apparently neither agency has comprehensive policy and procedures documents or guidelines.
### Table 4.9
Challenges and issues that face QPS and ADP and what initiatives and activities do they use to manage them

<table>
<thead>
<tr>
<th>#</th>
<th>Challenge or issue</th>
<th>Initiatives and activities that the agency uses to manage the identified challenge or issue</th>
<th>QPS (Queensland)</th>
<th>ADP (Abu Dhabi)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Training and resources</td>
<td>QPS staff members are provided with sufficient training to familiarize them with the types of investigations the unit is responsible for; also they undertake other training courses.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>Updating expertise</td>
<td>Attend regular industry seminars, do on job training, liaison with external agencies and industry, and attend national and international conferences and meetings.</td>
<td></td>
<td>No foreign expertise available to assist the unit in investigating computer crime, and only depends on the available staff.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>Cooperation with other organization or law enforcement</td>
<td>Regular contact and cooperation with other members from State, Federal and other law enforcement agencies nationally and internationally, and with commonwealth authorities and industry bodies.</td>
<td></td>
<td>National collaboration between the States, and attend the international conferences.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d</td>
<td>Jurisdictional problems of computer crime</td>
<td>Interstate and international cooperation to overcome this issue.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e</td>
<td>Anonymity services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Coping with computer crime legislation that differs between countries</td>
<td>Interstate and international cooperation to overcome this issue.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>f</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: dash (-) means no answer

This analysis showed that ADP and QPS approaches have a number of similar challenges and issues. The study indicated that there are some important issues that continue to create problems for the law enforcement agencies such as sufficient resources, and coping with computer crime legislation that differs between countries (jurisdictional issues, cooperation and communication problems between countries).

We found that the participants, especially ADP participants, sometimes gave disparate answers for the same questions. This presents a significant need for comprehensive and formal policy and procedures documents with regard to the investigation of computer crime. The study also highlights the importance of providing appropriate ongoing education and training for the staff to keep them updated with emerging crimes. Overall, the study identified areas where
improvements are needed and also identified the existing challenges and issues that require attention by the QPS and ADP in order to combat computer crime effectively. In fact, similar considerations should apply elsewhere in the world, and the results of the study are therefore also of relevance on the wider international front.

The next chapter examines the extent of money laundering over the last decade or so in Australia, the UAE, the UK and the USA. It presents a comprehensive cross-jurisdictional analysis of the figures representing the extent of money laundering in these four countries.
Chapter 5
The Extent of Money Laundering

Money laundering has been transformed in the past decade or less by the Internet, giving rise to the new term cyber-laundering. Lovet (2009) [25] entirely captures the nature of this transformation when he refers to the Internet as the big cyber-laundering machine. While it is clear that some money laundering does not constitute cybercrime in the traditional sense of the term, it is also clear that money laundering implemented via the Internet — cyber-laundering — does. Indeed, in some countries, including the UAE, money laundering that happens over the Internet is specifically criminalised under cybercrime legislation. This chapter examines the extent of money laundering over the last decade in four developed and fast-developing countries, Australia, UAE, the UK and the USA, four countries that represent a spectrum of economic development and culture. It does so with a view to understanding their anti-money laundering systems and their recent efforts to improve the effectiveness of those systems. In the case of the UAE, this chapter also refers to the cultural influences, discussed in more detail in Chapter 6, that differentiate it from the other three countries and which have, necessarily, been a factor in shaping those efforts and their current system. This chapter analyses and compares the estimates of the extent of money laundering in these countries, using estimates and information from various national and international agencies and researchers. It also analyses the number of Suspicious Activity Reports (SARs) lodged within each of these four countries, and the number of money laundering related court cases, prosecutions and convictions.

Overall, Chapter 5 addresses the following research question:
Q3. To what extent does the extent of money laundering in Australia, the UAE, the UK and the USA differ and how has it changed over time?

The first section of Chapter 5 analyses the published estimates of the extent of the money laundering in Australia, the UAE, the UK and the USA. Section 5.2 summarizes the reporting requirements in the four countries, and analyses and compares the numbers of SARs recorded and the number of money laundering cases prosecuted in each country. Section 5.3 discusses the findings of the chapter and the influence of local factors on the AML/CFT regimes. Section 5.4 presents our conclusions.

The work described in this chapter has been published in the following conference paper:


5.1 Money Laundering Estimates

Section 5.1 of this chapter studies a variety of estimations of the extent of money laundering in Australia, the UAE, the UK and the USA. It intends to compare how the estimates of money laundering in these four countries compare and how they are related to the International Monetary Fund estimates of 2 to 5 per cent of the GDP.

The illegal nature of money laundering makes it very difficult to measure accurately the amount of money laundered every year around the world. However, it is clearly important to try to do so. Though the FATF [247] has indicated that it does not publish any money laundering statistics, because it is impossible to produce a reliable estimation of the amount of money laundered, there are other existing national and international estimations that do provide some relevant figures. According to the FATF [248], one Australian Government Agency estimated that AU$2–3 billion annually is laundered through Australia. Global estimates range from US$300 billion to US$1,000 billion of funds laundered annually around the world [249, 250]. The IMF has estimated that the global amount of laundered money is the
equivalent of between 2 to 5 per cent of the world’s gross domestic product (GDP) [26]. Camdessus [26], Managing Director of the IMF, indicates that:

_While we cannot guarantee the accuracy of our figures ... the estimates of the present scale of money laundering transactions are almost beyond imagination — 2 to 5 percent of global GDP would probably be a consensus range. This scale poses two sorts of risks: one prudential, the other macroeconomic. Markets and even smaller economics can be corrupted and destabilized._

The UN Office on Drugs and Crime [251] adopts these estimates of the IMF; Beare and Schneider [252] note that the FATF and the Council of Europe and the UN do likewise. Table 5.1 lists several estimations of the value and extent of money laundering worldwide.

Table 5.1
Estimations of the extent of money laundering in the world annually

<table>
<thead>
<tr>
<th>Publication year</th>
<th>Estimation year</th>
<th>Estimation of global money laundering</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1998</td>
<td>1997</td>
<td>US$ 300–500 billion</td>
<td>USA Department of State [254]</td>
</tr>
<tr>
<td>1998</td>
<td>1998</td>
<td>2–5% of the global GDP</td>
<td>Michel Camdessus, IMF [26]</td>
</tr>
<tr>
<td>2002</td>
<td>1998</td>
<td>US$ 800 billion to US$ 1.5 trillion</td>
<td>Simon Maylam [255]</td>
</tr>
<tr>
<td>2009</td>
<td>1998</td>
<td>2–5% of the global GDP</td>
<td>UNODC [259]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US$ 800 billion to US$ 2 trillion</td>
<td></td>
</tr>
</tbody>
</table>

<sup>11</sup> In 2008, for example, AU$1 = US$0.95, therefore, AU$1.5 trillion * 0.95 = US$1.425 trillion. The exchange rate from www.xe.com based on the conversion rate on the 1st of July, 2008.
In line with the IMF approach, Table 5.2 illustrates the extent of money laundering using the lower and upper bounds of 2 to 5 per cent of a country's GDP to estimate the extent of money laundering in Australia, the UAE, the UK and the USA. Clearly, there is a huge difference between 2 and 5 per cent of the GDP. For instance, in 2008, the USA's GDP was about US$14,264 billion and 2 per cent of the GDP would be US$285 billion, while 5 per cent of the GDP would be US$713 billion. While 5 per cent of the GDP is an enormous amount of money, 2 per cent still points to a significant problem that needs to be addressed. It is interesting to note that the estimation of 2 per cent for money laundering of the USA's GDP is more than the UAE's GDP at any time in the past 10 years. Ultimately, regardless of the estimated percentage being suggested, the extent of money laundering is still in the billions of dollars range.

While the IMF estimates of money laundering based on 2 to 5 per cent of the GDP are useful, that range is very broad and there is clearly a need to find other alternative and more accurate estimates of the value and extent of the money laundering in the four countries. Therefore, we have conducted an analysis of the published estimates of money laundering worldwide and Tables 5.3 to 5.6 present a selection of the estimates that detail the value and extent of money laundering in these countries. Tables 5.3 to 5.6 indicate whether or not the estimation is within the IMF estimates of 2 to 5 per cent of the GDP, in addition to specifying the type of the estimation and the methods used to produce it.

Table 5.3 presents estimates made by various sources for Australia. These estimates account for between 0.21 and 12 per cent of Australia’s GDP. Each estimate represents less than 2 per cent of the GDP, except for one, and that estimate is itself a range of 4 to 12 per cent of the GDP. The findings show that none of the estimates of money laundering mentioned in Table 5.3 falls within the IMF range of 2 to 5 per cent of the GDP, although the 4 to 12 per cent estimate does reflect an overlap.
5.1 Money Laundering Estimates

Table 5.2
Estimations of the extent of money laundering in Australia, the UAE, the UK and the USA, 1999–2008, based on the GDP

<table>
<thead>
<tr>
<th>Year</th>
<th>Australia GDP in Billions US$</th>
<th>2% of GDP</th>
<th>5% of GDP</th>
<th>UAE GDP in Billions US$</th>
<th>2% of GDP</th>
<th>5% of GDP</th>
<th>UK GDP in Billions US$</th>
<th>2% of GDP</th>
<th>5% of GDP</th>
<th>USA GDP in Billions US$</th>
<th>2% of GDP</th>
<th>5% of GDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1999</td>
<td>401.998</td>
<td>8.04</td>
<td>20.1</td>
<td>55.181</td>
<td>1.1</td>
<td>2.76</td>
<td>1,502.89</td>
<td>30.06</td>
<td>75.14</td>
<td>9,268.43</td>
<td>185.37</td>
<td>463.42</td>
</tr>
<tr>
<td>2000</td>
<td>389.956</td>
<td>7.8</td>
<td>19.5</td>
<td>70.221</td>
<td>1.4</td>
<td>3.51</td>
<td>1,480.53</td>
<td>29.61</td>
<td>74.03</td>
<td>9,816.98</td>
<td>196.34</td>
<td>490.85</td>
</tr>
<tr>
<td>2001</td>
<td>368.123</td>
<td>7.36</td>
<td>18.41</td>
<td>68.677</td>
<td>1.37</td>
<td>3.43</td>
<td>1,471.40</td>
<td>29.43</td>
<td>73.57</td>
<td>10,127.95</td>
<td>202.56</td>
<td>506.4</td>
</tr>
<tr>
<td>2002</td>
<td>412.914</td>
<td>8.26</td>
<td>20.65</td>
<td>75.892</td>
<td>1.52</td>
<td>3.79</td>
<td>1,614.70</td>
<td>32.29</td>
<td>80.73</td>
<td>10,469.60</td>
<td>209.39</td>
<td>523.48</td>
</tr>
<tr>
<td>2003</td>
<td>527.76</td>
<td>10.56</td>
<td>26.39</td>
<td>88.959</td>
<td>1.78</td>
<td>4.45</td>
<td>1,862.77</td>
<td>37.26</td>
<td>93.14</td>
<td>10,960.75</td>
<td>219.22</td>
<td>548.04</td>
</tr>
<tr>
<td>2004</td>
<td>640.573</td>
<td>12.81</td>
<td>32.03</td>
<td>107.304</td>
<td>2.15</td>
<td>5.37</td>
<td>2,199.25</td>
<td>43.99</td>
<td>109.96</td>
<td>11,685.93</td>
<td>233.72</td>
<td>584.3</td>
</tr>
<tr>
<td>2005</td>
<td>713.262</td>
<td>14.27</td>
<td>35.66</td>
<td>135.198</td>
<td>2.7</td>
<td>6.76</td>
<td>2,280.06</td>
<td>45.6</td>
<td>114</td>
<td>12,421.88</td>
<td>248.44</td>
<td>621.09</td>
</tr>
<tr>
<td>2006</td>
<td>755.21</td>
<td>15.1</td>
<td>37.76</td>
<td>164.165</td>
<td>3.28</td>
<td>8.21</td>
<td>2,435.70</td>
<td>48.71</td>
<td>121.78</td>
<td>13,178.35</td>
<td>263.57</td>
<td>658.92</td>
</tr>
<tr>
<td>2007</td>
<td>909.743</td>
<td>18.19</td>
<td>45.49</td>
<td>180.18</td>
<td>3.6</td>
<td>9.01</td>
<td>2,803.40</td>
<td>56.07</td>
<td>140.17</td>
<td>13,807.55</td>
<td>276.15</td>
<td>690.38</td>
</tr>
<tr>
<td>2008</td>
<td>1,010.70</td>
<td>20.21</td>
<td>50.53</td>
<td>260.141</td>
<td>5.2</td>
<td>13.01</td>
<td>2,674.09</td>
<td>53.48</td>
<td>133.7</td>
<td>14,264.60</td>
<td>285.29</td>
<td>713.23</td>
</tr>
</tbody>
</table>

Source: Gross domestic product (GDP), current prices, from the IMF [109], World Economic Outlook Database, April 2009. The USA’s GDP and the UAE’s GDP for 2008 are estimations according to the IMF.
In the case of the UAE, a developing country, it has been difficult to find estimates of the value and extent of money laundering. However, Table 5.4 outlines the findings of one estimate of money laundering in the UAE. According to this table, the amount of money laundered annually in the UAE is around US$1 billion, which represents 1.32 per cent of the UAE’s GDP. This figure is still lower than the IMF 2 to 5 per cent range of the GDP. However, because it is the only figure available, it is difficult on this basis to generalize to the value and extent of money laundering in the UAE.

In contrast to the estimates of money laundering in Australia and the UAE, some estimates of money laundering in the UK and the USA fall within the IMF estimates of 2 to 5 per cent of the GDP. Wakefield [260] presents an estimate of US$300 billion of money laundering in the USA, which represents 3.06 per cent of the USA’s GDP. Table 5.5 presents estimates of money laundering in the USA derived from various sources. These estimates indicate that money laundering in the USA ranges from 0.40 to 33 per cent of the GDP. One estimate is a range that accounts for between 4 and 33 per cent of the GDP. There is a huge difference between 4 and 33 per cent. For instance, in 2008, the USA’s GDP was around US$14,264 billion and 33 per cent of the GDP would be US$4707 billion; this represents a significant amount that is difficult to comprehend.

The UK HM Customs and Excise estimates of money laundering in the UK fall within the IMF estimate of 2 to 5 per cent of the GDP. Table 5.6 presents some national agency and academic estimates of the value and extent of money laundering in the UK. According to these estimates, money laundering accounts for anywhere between 0.29 and 15 per cent of the UK’s GDP.

The findings show that there are some significant variations in the estimates of the value and extent of money laundering: no doubt a reflection of the type of methods used to produce such estimations. Nevertheless, it seems clear that there are significant variations in the value and extent of money laundering in Australia, the UAE, the UK and the USA. While the FATF assessment team found that Australia and the UAE are less compliant with its recommendations [248, 261], our analysis shows that the estimates of the amount of money laundered in those two countries are less than those found in the UK and the USA.
Table 5.3

Estimations of the amount of laundered money in Australia

<table>
<thead>
<tr>
<th>Publication year</th>
<th>Estimation year</th>
<th>ML estimation (in billions of US$ or percentage of GDP)</th>
<th>GDP (in billions of US$)</th>
<th>ML Percentage of GDP</th>
<th>Within the IMF range of 2–5% of GDP</th>
<th>Type of estimation (per year or for specific year)</th>
<th>Type of methods used to develop the estimation</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>1995</td>
<td>US$2.59 billion(^{12}) (AUD 3.5 billion)</td>
<td>371.247</td>
<td>0.70%</td>
<td>X</td>
<td>For specific year, 1995</td>
<td>Crime statistics, surveys, interviews, AUSTRAC data, financial reports and a range of crime categories</td>
<td>John Walker [253]</td>
</tr>
<tr>
<td>1997</td>
<td></td>
<td>4–12% of GDP</td>
<td>347.146</td>
<td>4–12%</td>
<td>X</td>
<td>Per year</td>
<td>Micro-economic estimates by crime category based on sampling, detailed medical, social and financial/tax records</td>
<td>Peter Quirk [262]</td>
</tr>
<tr>
<td>2007</td>
<td>2004</td>
<td>US$3.15 billion(^{13}) (AU$4.5 billion)</td>
<td>640.573</td>
<td>0.49%</td>
<td>X</td>
<td>Per year</td>
<td>Based on the responses to the 1995 Walker report, annual reports and other statistics, surveys and interviews, other research and AUSTRAC data</td>
<td>AUSTRAC, John Walker and RMIT University [263]</td>
</tr>
<tr>
<td>2005</td>
<td></td>
<td>US$1.5–2.25 billion(^{14}) (AU$2–3 billion)</td>
<td>713.262</td>
<td>0.21–0.32%</td>
<td>X</td>
<td>Per year</td>
<td>N/A</td>
<td>FATF [248] citing one unidentified Australian Government Agency</td>
</tr>
<tr>
<td>2006</td>
<td></td>
<td>US$9.78 billion(^{15}) (AU$11.5 billion)</td>
<td>909.743</td>
<td>1.08%</td>
<td>X</td>
<td>Per year</td>
<td>Applying the IMF figure of 2–5% of GDP</td>
<td>Commonwealth of Australia [264]</td>
</tr>
<tr>
<td>2009</td>
<td></td>
<td>US$9.72 billion(^{16}) (AU$12 billion)</td>
<td>755.066</td>
<td>1.29%</td>
<td>X</td>
<td>Per year</td>
<td>N/A</td>
<td>Australian Crime Commission (ACC) [265]</td>
</tr>
</tbody>
</table>

Note: N/A means not available.


---

12 In 1995: AU$1 = US$0.74; therefore, AU$3.5 billion *0.74 = US$2.59 billion.
13 In 2004: AU$1 = US$0.7, therefore, AU$4.5 billion *0.7 = US$3.15 billion.
14 In 2005: AU$1 = US$0.75; therefore, AU$2 billion *0.75–3 billion *0.75 = US$1.5–2.25 billion.
15 In 2007: AU$1 = US$0.85; therefore, AU$11.5 billion *0.85 = US$9.78 billion.
### Table 5.4 Estimation of the amount of laundered money in the UAE

<table>
<thead>
<tr>
<th>Publication year</th>
<th>Estimation year</th>
<th>ML estimation (in billions of US$ or percentage of GDP)</th>
<th>GDP (in billions of US$)</th>
<th>ML Percentage of GDP</th>
<th>Within the IMF range of 2-5% of GDP</th>
<th>Type of estimation (per year or for specific year)</th>
<th>Type of methods used to develop the estimation</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td></td>
<td>US$1 billion</td>
<td>75.892</td>
<td>1.32%</td>
<td>X</td>
<td>Per year</td>
<td>N/A</td>
<td>International Crime Threat Assessment prepared by a USA Government Interagency Working Group [266]</td>
</tr>
</tbody>
</table>

Note: N/A means not available

Source: GDP, current prices, from the IMF [109], World Economic Outlook Database, April 2009.

### Table 5.5 Estimations of the amount of laundered money in the USA

<table>
<thead>
<tr>
<th>Publication year</th>
<th>Estimation year</th>
<th>ML estimation (in billions of US$ or percentage of GDP)</th>
<th>GDP (in billions of US$)</th>
<th>ML Percentage of GDP</th>
<th>Within the IMF range of 2-5% of GDP</th>
<th>Type of estimation (per year or for specific year)</th>
<th>Type of methods used to develop the estimation</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1993</td>
<td>1993</td>
<td>US$100 billion</td>
<td>6657.4</td>
<td>1.50%</td>
<td>X</td>
<td>Per year</td>
<td>N/A</td>
<td>USA Department of Treasury [267]</td>
</tr>
<tr>
<td>1997</td>
<td></td>
<td>4–33% of GDP</td>
<td>7072.22</td>
<td>4.33%</td>
<td>X</td>
<td>Per year</td>
<td>Peter Quirk [262]</td>
<td></td>
</tr>
<tr>
<td>1998</td>
<td>1998</td>
<td>US$34.6 billion</td>
<td>8746.97</td>
<td>0.40%</td>
<td>X</td>
<td>Per year</td>
<td>John Walker [256]</td>
<td></td>
</tr>
<tr>
<td>2000</td>
<td></td>
<td>US$300 billion</td>
<td>9,816.9</td>
<td>3.06%</td>
<td>√</td>
<td>Per year</td>
<td>N/A</td>
<td>Julie Wakefield [260]</td>
</tr>
<tr>
<td>2003</td>
<td>2002</td>
<td>US$123.4 billion</td>
<td>10,469.60</td>
<td>1.18%</td>
<td>X</td>
<td>For specific year, 2002</td>
<td>N/A</td>
<td>Indian Express Group [268]</td>
</tr>
<tr>
<td>2005</td>
<td></td>
<td>US$194.7 billion¹⁶ UK£110 billion</td>
<td>12421.8</td>
<td>1.57%</td>
<td>X</td>
<td>Per year</td>
<td>N/A</td>
<td>Yeandle et al. [269]</td>
</tr>
</tbody>
</table>

Note: N/A means not available

Source: GDP, current prices, from the IMF [109], World Economic Outlook Database, April 2009. The Exchange rate from www.xe.com based on the conversion rate on the first of July of the estimated year

¹⁶ In 2005: UK£1 = US$1.77, therefore, UK£110 billion *1.77 = US$194.7 billion.
### Table 5.6

Estimations of the amount of laundered money in the UK

<table>
<thead>
<tr>
<th>Publication year</th>
<th>Estimation year</th>
<th>ML estimation (in billions of US$ or percentage of GDP)</th>
<th>GDP (in billions of US$)</th>
<th>ML Percentage of GDP</th>
<th>Within the IMF range of 2-5% of GDP</th>
<th>Type of estimation (per year or for specific year)</th>
<th>Type of methods used to develop the estimation</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1997</td>
<td>1997</td>
<td>1–15% of GDP</td>
<td>1061.382</td>
<td>1–15%</td>
<td>X</td>
<td>Per year</td>
<td>Micro-economic approach which build up estimates by crime category based on sampling, street knowledge, detailed medical, social and financial/tax records</td>
<td>Peter Quirk [262]</td>
</tr>
<tr>
<td>2002</td>
<td>1998</td>
<td>US$4.18 billion UK£2.5 billion</td>
<td>1456.155</td>
<td>0.29%</td>
<td>X</td>
<td>For specific year, 1998</td>
<td>N/A</td>
<td>Simon Maylam [255]</td>
</tr>
<tr>
<td>1998</td>
<td>1998</td>
<td>7.4% of GDP</td>
<td>1456.155</td>
<td>7.40%</td>
<td>X</td>
<td>Per year</td>
<td>Using crime and economic statistics and Transparency International’s Corruption Index</td>
<td>John Walker [256]</td>
</tr>
<tr>
<td>2001</td>
<td>1998</td>
<td>US$11.36 billion UK£8 billion</td>
<td>1,471.4</td>
<td>0.77%</td>
<td>X</td>
<td>Per year</td>
<td>N/A</td>
<td>Saeed Shah, The Independent [270]</td>
</tr>
<tr>
<td>2005</td>
<td>2007</td>
<td>2–5% of GDP UK£19-48 billion</td>
<td>2,199.2</td>
<td>2–5%</td>
<td>√</td>
<td>Per year</td>
<td>Using the IMF figure (2–5% of GDP) to estimate the amount of money laundered in the UK</td>
<td>UK HM Treasury [271]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2–5% of GDP UK£23–57 billion</td>
<td>2803.404</td>
<td>2–5%</td>
<td>√</td>
<td>Per year</td>
<td>The Financial Services Authority (FSA) applied the same figure that was being used by the HM Customs and Excise and the IMF (2–5% of GDP) to estimate the amount of money laundered in the UK</td>
<td>Financial Services Authority (FSA) [272]</td>
</tr>
</tbody>
</table>

**Note:** N/A means not available

Source: GDP, current prices, from the IMF [109], World Economic Outlook Database, April 2009. The Exchange rate from www.xe.com based on the conversion rate on the first of July of the estimated year.

---

17 In 1998: UK£1 = US$1.67, therefore, UK£2.5 billion *1.67 = US$4.18 billion.
18 In 2001: UK£1 = US$1.42, therefore, UK£8 billion *1.42 = US$11.36 billion.
5.2 Anti-money Laundering Statistics: Suspicious Activity Reports (SARs) and Cases, Prosecutions and Convictions

This section discusses the number of SARs submitted that is of interest as a secondary indicator of the extent of the money laundering and the effectiveness of the money laundering investigation regimes. It concludes with a discussion on the number of money laundering cases, prosecutions and convictions in the four countries.

5.2.1 Reporting Requirements and SARs

Many jurisdictions require financial institutions (for example, banks) and certain non-financial institutions (for instance, insurance companies) to provide several types of reports, such as large cash transaction reports and suspicious activity reports. These reports are collected by the FIU in each country, which is then responsible for analyzing that data and investigating any potential money laundering. As mentioned in Chapter 2, all four countries require the reporting of certain cash and international transactions and also require the reporting of suspicious financial activities through the lodgement of SARs. FATF Recommendation 13 and Special Recommendation IV relate to the reporting of suspicious activities concerning money laundering and the financing of terrorism. While the UK is fully compliant with those Recommendations [273], Australia [248] and the USA [274] are largely compliant with them; the UAE is non-compliant with both [261]. There are, therefore, some variations to be expected in the number of SARs recorded in these four countries.

In contrast to the USA, Australia, the UAE and the UK have no minimum thresholds if there are some reasonable grounds for treating the transaction as suspicious. The UAE legislation does not specify what types of activities could be considered suspicious transactions. These differences between the four countries in having different interpretations of the types of suspicious transactions would be expected to affect some variations in the number of the SARs. Table 5.7 compares the SARs identification criteria used in Australia, the UAE, the UK and the USA, based on criteria from the FATF definition of SARs. The FATF has evaluated the AML/CFT systems of Australia, the UAE, the UK and the USA in 2005, 2007, 2006 and 2006, respectively.
Table 5.7 also illustrates compliance with the FATF Recommendation 13 and Special Recommendation IV on reporting suspicions activities concerning money laundering and the financing of terrorism. While the UK is fully compliant with those recommendations, Australia and the USA are largely compliant with them. In contrast, the UAE is non-compliant with both recommendation 13 and special recommendation IV.

The level of SARs received in Australia, the UAE, the UK and the USA varies and that may well be caused by the difference in the size of the economy in each country in addition to other factors, such as the SARs criteria already referred to. Table 5.8 presents the number of received SARs from 1999 to 2008 in each country. The highlighted areas in the table show massive increases compared to previous years. This may be explained by the introduction of the FATF Special Recommendations on countering the financing of terrorism in 2001 and the introduction of the FATF 2003 new standards including extending AML reporting to non-financial institutions, such as lawyers and real estate agents [175]. For Australia and the UAE, it seems there is a relation between the increase in the number of SARs and the FATF mutual evaluations in 2005 and 2007, respectively.

Table 5.8 shows the number of SARS for each 1,000 in the population and the number of SARs per unit (billions of dollars) of the GDP. Generally, the number of SARS, SARs per 1,000 of population and SARs per unit of GDP is steadily increasing in the aforesaid countries. Figures 5.3 and 5.4 demonstrate the number of SARs per 1,000 of population and the number of SARs per unit of the GDP in Australia, the UAE, the UK and USA from 1999 to 2008. While the number of SARs is invariably increasing, the number of SARs per 1,000 of population is very low in Australia and the UAE compared to the UK and the USA in the period between 2003 and 2008. It was also observed that the number of SARs per unit of the GDP in Australia is less than in the UK and the USA. Lastly, the number of SARs per unit of GDP in the UAE is less than those in the above countries and does not reflect the size of the country’s economy.
<table>
<thead>
<tr>
<th>Suspicious activity reports (SARs)/ Suspicious transaction reports (STRs)</th>
<th>FATF Criteria</th>
<th>Australia Compliance with FATF</th>
<th>UAE Compliance with FATF</th>
<th>UK Compliance with FATF</th>
<th>USA Compliance with FATF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Money laundering</td>
<td>Reasonable grounds to suspect that the transaction: (i) may be relevant to investigation of an evasion, or attempted evasion of a taxation law; or (ii) may be relevant to investigation of, or prosecution of a person for, an offence against a law of the Commonwealth or of a Territory; or (iii) may be of assistance in the enforcement of the Proceeds of Crime Act 1987, Proceeds of Crime Act 2002 or the regulations made under these Acts</td>
<td>Largely compliant with R.13</td>
<td>Non-compliant with R.13</td>
<td>Compliant with R.13</td>
<td>Largely compliant with R.13</td>
</tr>
<tr>
<td></td>
<td>Detect known or suspected violation of Federal law or a suspicious transaction related to a money laundering activity or a violation of the BSA: (1) Insider abuse involving any amount (2) Violations aggregating $5,000 or more where a suspect can be identified (3) Violations aggregating $25,000 or more regardless of potential suspects (4) Transactions aggregating $5,000 or more that involve potential money laundering or violate the Bank Secrecy Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financing terrorism</td>
<td>Reasonable grounds to suspect that the transaction is preparatory to the commission of a financing terrorism offence or may be relevant to investigation of or the prosecution of a person for financing a terrorism offence</td>
<td>Largely compliant with SR.IV</td>
<td>Suspicous transactions related to financing of terrorism</td>
<td>Non-compliant with SR.IV</td>
<td>Compliant with SR.IV</td>
</tr>
<tr>
<td></td>
<td>Knows or suspects, or (b) has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes: 1. FATF requires reporting of all suspicious transactions regardless of amount involved. 2. Australia, the UAE and the UK are consistent with FATF. 3. USA have a threshold of at least USD 5,000 (money services businesses have threshold of at least USD 2,000) to fill SARs.

### Table 5.8

SARs received in Australia, the UAE, the UK and the USA, 1999–2008

<table>
<thead>
<tr>
<th>Year</th>
<th>Australia</th>
<th></th>
<th></th>
<th>UAE</th>
<th></th>
<th></th>
<th>UK</th>
<th></th>
<th></th>
<th>USA</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SARs</td>
<td>SARs/1,000 Population</td>
<td>SARs per unit of GDP</td>
<td>SARs</td>
<td>SARs/1,000 Population</td>
<td>SARs per unit of GDP</td>
<td>SARs</td>
<td>SARs/1,000 Population</td>
<td>SARs per unit of GDP</td>
<td>SARs</td>
<td>SARs/1,000 Population</td>
<td>SARs per unit of GDP</td>
</tr>
<tr>
<td>1999</td>
<td>6,541</td>
<td>0.35</td>
<td>16.27</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>15,115</td>
<td>0.26</td>
<td>10.06</td>
<td>120,941</td>
<td>0.43</td>
<td>13.05</td>
</tr>
<tr>
<td>2000</td>
<td>7,068</td>
<td>0.37</td>
<td>18.13</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>18,447</td>
<td>0.31</td>
<td>12.46</td>
<td>163,184</td>
<td>0.58</td>
<td>16.62</td>
</tr>
<tr>
<td>2001</td>
<td>7,247</td>
<td>0.37</td>
<td>19.69</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>29,976</td>
<td>0.51</td>
<td>20.37</td>
<td>204,915</td>
<td>0.72</td>
<td>20.23</td>
</tr>
<tr>
<td>2002</td>
<td>7,809</td>
<td>0.4</td>
<td>18.91</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>56,023</td>
<td>0.94</td>
<td>34.7</td>
<td>281,373</td>
<td>0.98</td>
<td>26.88</td>
</tr>
<tr>
<td>2003</td>
<td>8,054</td>
<td>0.4</td>
<td>15.26</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>94,708</td>
<td>1.59</td>
<td>50.84</td>
<td>507,217</td>
<td>1.75</td>
<td>46.28</td>
</tr>
<tr>
<td>2004</td>
<td>11,484</td>
<td>0.57</td>
<td>17.93</td>
<td>290</td>
<td>0.08</td>
<td>2.7</td>
<td>154,536</td>
<td>2.58</td>
<td>70.27</td>
<td>689,414</td>
<td>2.35</td>
<td>59</td>
</tr>
<tr>
<td>2005</td>
<td>17,212</td>
<td>0.84</td>
<td>24.13</td>
<td>301</td>
<td>0.07</td>
<td>2.23</td>
<td>195,702</td>
<td>3.25</td>
<td>85.83</td>
<td>919,230</td>
<td>3.11</td>
<td>74</td>
</tr>
<tr>
<td>2006</td>
<td>24,801</td>
<td>1.2</td>
<td>32.84</td>
<td>556</td>
<td>0.13</td>
<td>3.39</td>
<td>213,561</td>
<td>3.52</td>
<td>87.68</td>
<td>1,078,894</td>
<td>3.61</td>
<td>81.87</td>
</tr>
<tr>
<td>2007</td>
<td>24,440</td>
<td>1.16</td>
<td>26.86</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>220,484</td>
<td>3.62</td>
<td>78.65</td>
<td>1,250,439</td>
<td>4.15</td>
<td>90.56</td>
</tr>
<tr>
<td>2008</td>
<td>29,089</td>
<td>1.36</td>
<td>28.78</td>
<td>13,101</td>
<td>2.75</td>
<td>50.36</td>
<td>210,524</td>
<td>3.45</td>
<td>78.73</td>
<td>1,290,590</td>
<td>4.24</td>
<td>90.48</td>
</tr>
</tbody>
</table>

Source: AUSTRAC: AUSTRAC Annual Reports 2001–02 [275], 2003–04 [276] and 2007–08 [277]; FATF [261], Hamdan [278]; SOCA, The Suspicious Activity Reports Regime: Annual Report 2007 [279] and Annual Report 2008 [280], Matthew Fleming [281], Jackie Harvey [282]; FinCEN [283]: The SAR Activity Review - By the Numbers; Population & GDP, current prices, from the IMF [109], World Economic Outlook Database, April 2009. The USA’s GDP and the UAE’s GDP and population for 2008 are estimations according to the IMF. FinCEN and SOCA refer to their suspicious activity reports as SARS, however, AUSTRAC and AMLSCU refer to their SARS as SUSTRs and STRs, respectively. Also, in some countries, SARS are counted based on a financial year, but assigned in this Table to a calendar year, for instance, 1998–99, which means 1999 in the Table.

19 Number of SARS from 2004 to 2006 is collected from the FATF (2008) and for 2008 from Hamdan (2009).
Figure 5.1 Number of SARs per 1,000 of the population in Australia, UAE, the UK and the USA, 1999–2008

Figure 5.2 Number of SARs per unit (billions of dollars) of GDP in Australia, UAE, the UK and the USA, 1999–2008
5.2.2 Anti-money Laundering Statistics: Cases, Prosecutions and Convictions

To examine the effectiveness of the AML/CFT regimes used in Australia, the UAE, the UK and the USA, our study has attempted to identify the number of money laundering cases, prosecutions and convictions in each country. However, there were some difficulties in finding the statistics for the money laundering prosecutions and convictions in the four countries over the same period of time. In fact, the FATF [248] noted that the lack of statistics on Australian States and Territories prosecutions and convictions for offences of money laundering undermines a precise evaluation of the effectiveness of the Australia AML/CFT regime. Also, the FATF [261] indicated that, generally, in the UAE, detection and statistical analysis of money laundering cases is not effective. That could be a result of not providing a clear definition of the types of suspicious transactions. Having said that, some useful information about money laundering prosecutions and convictions in the four countries has been gathered and is presented below.

Between 2000 and 2005, there were 51 charges of money laundering in Australia under the Proceeds of the Crime Act and the Criminal Code Act (Cth) [179]. Also, the Australian Institute of Criminology cited that between January 2003 and January 2008, the Commonwealth Director of Public Prosecutions dealt with 77 charges of money laundering offences, and 35 individuals were convicted in 46 of the 77 charges [179]. In the UAE, between 2002 and June 2009, there were 285 money laundering cases sent to the Public Prosecutions Office, with 20 out of the 285 cases being sent to the courts [278]. In the USA, between 1994 and 2001, about 18,500 defendants were charged with money laundering with at least one of the charges besides other offences, and 10,610 of these were charged with money laundering as the most serious offence [284]. Also, from 2006 to 2008, 6,204 money laundering and Bank Secrecy Act (BSA) investigations that were initiated, resulted in 5,014 recommended prosecutions and 3,243 custodial sentences [285]. With regard to the UK, from 1999 to 2007, there were 7,569 money laundering prosecutions that resulted in 3,796 convictions (Harvey [282] and the UK Director of Public Prosecutions [286]). Table 5.9 summarizes these statistics in Australia, the UAE, the UK and the USA.
Table 5.9
Money laundering prosecutions and convictions in the Australia, the UAE, the UK and the USA

<table>
<thead>
<tr>
<th>Country</th>
<th>Period of time</th>
<th>ML prosecutions/cases</th>
<th>ML convictions</th>
<th>Percentage of ML convictions (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>2000–2005</td>
<td>N/A</td>
<td>51</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2003–2008</td>
<td>N/A</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>UAE</td>
<td>2002–2008</td>
<td>285</td>
<td>20</td>
<td>7.02</td>
</tr>
<tr>
<td>UK</td>
<td>1999–2007</td>
<td>7,569</td>
<td>3,796</td>
<td>50.15</td>
</tr>
<tr>
<td>USA</td>
<td>1994–2001</td>
<td>N/A</td>
<td>18,500</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2006–2008</td>
<td>6,204</td>
<td>3,243</td>
<td>52.27</td>
</tr>
</tbody>
</table>

Note: N/A means not available

Table 5.10 illustrates detailed information in relation to money laundering prosecutions and convictions per year in the UK from 1999 to 2007. Similarly detailed information for the other three countries has not been identified.

Table 5.10
Money laundering prosecutions and convictions in the UK, 1999–2007

<table>
<thead>
<tr>
<th>Year</th>
<th>Prosecutions</th>
<th>Convictions</th>
<th>Percentage of ML convictions (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1999</td>
<td>126</td>
<td>39</td>
<td>30.95</td>
</tr>
<tr>
<td>2000</td>
<td>129</td>
<td>50</td>
<td>38.76</td>
</tr>
<tr>
<td>2001</td>
<td>182</td>
<td>75</td>
<td>41.21</td>
</tr>
<tr>
<td>2002</td>
<td>256</td>
<td>86</td>
<td>33.59</td>
</tr>
<tr>
<td>2003</td>
<td>300</td>
<td>123</td>
<td>41</td>
</tr>
<tr>
<td>2004</td>
<td>552</td>
<td>207</td>
<td>37.5</td>
</tr>
<tr>
<td>2005</td>
<td>1,327</td>
<td>595</td>
<td>44.84</td>
</tr>
<tr>
<td>2006</td>
<td>2,379</td>
<td>1,273</td>
<td>53.51</td>
</tr>
<tr>
<td>2007</td>
<td>2,318</td>
<td>1,348</td>
<td>58.15</td>
</tr>
</tbody>
</table>

Source: 1999–2002 from Jackie Harvey [282], as of 2003–2007 from the UK Director of Public Prosecutions [286].

As can be seen in Table 5.10, the number of money laundering prosecutions and convictions in the UK is steadily increasing every year. It also shows that the conviction rate for the last few years has steadily increased to reach 58.15 per cent in 2007, which indicates that an effective AML/CFT regime is being used and implemented in the UK.
5.3 Discussion

In this section, we discuss our findings and relate them to the influence of the local factors in the local AML/CFT regimes of the four countries to better understand both the extent of the success of the current approaches for combating money laundering and the problems remaining to be addressed.

The findings indicate that there are some important variations in the estimates of the extent of money laundering in Australia, the UAE, the UK and the USA. The estimates of the laundered money in Australia account for 0.21 to 12 per cent of the GDP. In the UAE, the estimate of the laundered money annually is about US$ 1 billion, which represents 1.32 per cent of the GDP. These estimates do not conform with the IMF estimate range of 2 to 5 per cent of the GDP. On the other hand, some estimates of money laundering in the UK and the USA do fall within the IMF estimates.

There is, likewise, a variation in the level of SARs received in Australia, the UAE, the UK and the USA that may well be caused by the difference in the size of the economy in each country in addition to other factors, such as the reporting criteria already referred to. The number of SARS, both the SARs per 1,000 of population and the SARs per unit of the GDP, is increasing in Australia, the UAE, the UK and the USA. The findings indicate that the number of SARs per unit of the GDP in Australia and the UAE are less than in the UK and the USA. During the FATF mutual evaluation of the AML/CFT system of the UAE, in 2007, the FATF found that the UAE is non-compliant with Recommendation 13 and the Special Recommendation IV concerning suspicious transaction reporting and also, only partially compliant with Recommendation 32 about maintaining comprehensive statistics including money laundering cases and SARs. On the other hand, Australia and the USA are largely compliant with these Recommendations. The UK is fully compliant with Recommendation 13 and largely compliant with Recommendation 32 and Special Recommendation IV. Non-compliance with the FATF Recommendations on the implementation of the suspicious reporting regime and maintaining statistics could partially explain why the UAE’s AML/CFT regime produces a smaller number of SARs. The FATF’s evaluation feedback on the UAE’s AML/CFT regime could also explain why, in recent years, the number of SARs in
the UAE has increased rapidly, reaching 13,101 reports in 2008 [278]. This could represent a quick response to the FATF evaluation of the UAE AML/CFT system.

Table 5.9 shows that more than 50 per cent of the money laundering cases in the UK and the USA have resulted in successful convictions. The conviction rate in the UAE is very low, representing about 7 per cent of all money laundering cases within the period 2002 to 2008.

Chapter 6 analyzes in detail the extent of compliance of the AML/CFT regimes of these four countries with the FATF Recommendations. That work, amongst others, identifies and analyzes the influence of the local factors on the local AML/CFT regimes and their FATF compliance. We present a summary of the findings of that work here.

Our findings show that the FATF needs to consider the distinct culture of a country whether developed or developing, when evaluating its AML/CFT system. Cultural factors are an important determinant of a country’s regulations and the character of its financial systems, and it is not surprising that those founding members of the FATF, such as Australia, the UK and the USA, may have left their cultural imprints on this organization. The UAE has not participated in the development of the FATF Recommendations; it has a different culture to the other three countries, religion is a dominating influence, and citizens have some other, very strongly shared values, some of which are not characteristic of developed countries, such as extended families and belonging to the same tribe [287]. These various cultural and religious factors have impacted on how the UAE has implemented its regulations and financial system and, accordingly, its AML/CFT system.

In the UAE, there are, for example, simple things such as carrying large sums of cash and purchasing properties and expensive products in cash, something which is regarded as normal [261]. A more fundamental example is provided by the Hawala system that has been in use since time immemorial in the Middle East to transfer money or value between the people in a local community. There has been much discussion about the challenges and problems that the Hawala system poses for the financial systems and its regulators. The main concern with the Hawala system has been that it was not regulated and, therefore, could be abused for
criminal purposes. The UAE has established regulations in relation to this system [288] and according to the Hawala Regulations System in the UAE, Hawaladars should register themselves and then become recognized as Hawala Brokers [288]. The Hawala Regulations in the UAE intend to ensure that the brokers and intermediaries provide details of money transfers (remitters and beneficiaries) and report any suspicious transfers. This is intended to regulate the system and protect it from abuse for illegal purposes, such as money laundering and the financing of terrorism. The FATF has indicated that the UAE step for addressing the informal Hawala system was a positive initiative and a strong lead internationally [261]. However, the FATF also noted that the registration is only voluntary and, therefore, the FIU of the UAE has no legal power to inspect Hawaladars for non-compliance with its requirements.

In terms of religion, Islam has a dominant influence in the UAE. Not only does Islam prohibit any activity funded by money derived from unlawful trade or ill-gotten property, but gains from gambling and bank interest are also prohibited [289]. However, this is normal practice in Australia, the UK and the USA. This means that the financial system in the UAE is very different from Australia, the UK and the USA. Kanatas and Stefanadis (2005) [290] have shown that development of a country’s legal system and financial systems are related to its religious beliefs. The findings show that these religious practices in the UAE have an impact on the implementation of its regulations and financial systems. In contrast, Australia, the UK and the USA are much less affected by such factors.

Other differences that differentiate the UAE from Australia, the UK and the USA are not only that the UAE is still a developing country, albeit developing very quickly, but also that the UAE does not impose income tax. Consequently, in the UAE, as in some other Middle East countries, money laundering for tax evasion is a non-issue.

5.4 Conclusion

This chapter has presented a comprehensive cross-jurisdictional analysis of the extent of money laundering in Australia, the UAE, the UK and the USA. While Australia has 19 different offences for money laundering, the UAE, the UK and the
USA each have only three separate offences that are considered to be money laundering. The chapter has investigated the value and extent of money laundering in these countries using estimates and information from various national and international agencies and researchers. Some estimates of money laundering in the UK and the USA fall within the IMF estimates of 2 to 5 per cent of the GDP, this is in contrast to estimates for Australia and the UAE.

The chapter has examined the process of the investigation of money laundering and the number of suspicious activity reports (SARs) received from 1999 to 2008 in Australia, the UAE, the UK and the USA. While the number of SARs is increasing in all four jurisdictions, the number of SARs per 1,000 of population is very low in Australia and the UAE compared to the UK and the USA in the period 2003–2008. The chapter has also outlined the number of money laundering prosecutions and convictions in those four countries.

In conclusion, Chapter 5 has found that there are considerable variations in the estimates of the extent of the amount of money laundered in these four countries. This has significant implications for policy makers, regulators and evaluators. Our overall conclusion is that cultural and religious differences impose a limit on the extent to which we can expect the universal harmonisation of anti-money laundering regimes, and to achieve the best success in anti-money laundering globally, the international community must take such differences into account — the difficulty is in the detail and, so too, must be the solution.

Chapter 6 expands the discussion on money laundering through examining how Australia, the UAE, the UK and the USA have interpreted and remained faithful to the FATF Recommendations on AML/CFT.
Chapter 6

Money Laundering and FATF Compliance by Australia, the UAE, the UK and the USA

Chapter 6 addresses the following research question:

Q4. To what extent do the anti-money laundering/combating the financing of terrorism regimes in Australia, the UAE, the UK and the USA differ with respect to their compliance to the international Financial Action Task Force (FATF) Recommendations and to what extent have local factors, such as cultural and economic factors, affected the UAE’s compliance with these recommendations and what improvements are needed?

Chapter 5 has examined the extent of money laundering over the last decade or so in Australia, the UAE, the UK and the USA. It found that some estimates of money laundering in the UK and the USA fall within the IMF estimates of 2 to 5 per cent of the GDP; this is in contrast to the estimates for Australia and the UAE. Chapter 5 also analysed the number of Suspicious Activity Reports (SARs) lodged within each of these four countries, and the number of money laundering related cases, prosecutions and convictions. Chapter 6 analyses the differences in the AML/CFT systems of Australia, the UAE, the UK and the USA, and the extent to which they have interpreted and remained faithful to the FATF Recommendations. The chapter makes use of the FATF evaluation reports for Australia, the UAE, the UK and the USA and compares their compliance and discusses the local factors, such as cultural and economic factors, that have arguably affected the UAE’s compliance with the FATF recommendations.
There are, generally speaking, two reasons why organisations and individuals may wish to launder money. First, in order to hide illegitimately acquired income or to avoid divulging activities which if closely scrutinized might reveal related illegal activities. Second, in order to hide legitimate income in order to avoid income tax in countries in which it is levied. If the extent of money laundering is extreme, then this represents a substantial threat to the revenue and economy of a country and possibly an untenable level of (probably organised) criminal activity. Therefore, it is in society’s interests to detect money laundering. The prevention of money laundering will arguably prevent the loss of government revenue and will likely prevent, or at least reduce, criminal activity.

Consequently, countries globally have legislated against money laundering. At the International level, the Financial Action Task Force (FATF) developed the 40+9 Recommendations on anti-money laundering and combating the financing of terrorism (AML/CFT) [176]. These 40+9 Recommendations are generally recognised as an international standard for implementing any AML/CFT system. Countries such as Australia, the UAE, the UK and the USA have reformulated their legislation and regulations to bring them into line with the FATF recommendations. Interestingly, these four countries, among others, have been identified by the USA Department of State as the major money laundering countries in 2008 [291].

The first section of this chapter analyses and compares the extent of the compliance in these countries with the FATF recommendations. It also discusses the implications for non-compliant countries. Section 6.2 analyses how cultural and other local factors have arguably affected the UAE’s compliance with the FATF recommendations. Section 6.3 presents our conclusions.

The work discussed in this chapter has been accepted in the following conference:

6.1 Compliance with the FATF 40+9 Recommendations

The FATF has evaluated the AML/CFT systems of many countries including Australia, the UAE\(^{20}\), the UK and the USA. Table 6.1 illustrates the year and number of evaluations for the AML/CFT systems for these four countries. This table shows clearly that each country’s AML/CFT system has been evaluated against the FATF Recommendations three times. However, the first two evaluations of each country’s AML system were based on only the FATF 40 Recommendations on combating money laundering. The third round of evaluation for each one of these four countries was based on the FATF 40+9 Recommendations on combating money laundering and the financing of terrorism. We focus here on analysing the result of the most recent evaluation of the AML/CFT systems of these countries.

### Table 6.1

<table>
<thead>
<tr>
<th>Year of evaluation</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1992</td>
<td>√</td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>1996</td>
<td>√</td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>2000</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2004</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>2007</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
</tbody>
</table>

Sources: for Australia from AUSTRAC [188]; for the UAE from FATF [261] and Roule and Kinsell [292]; for the UK from FATF [273] & [293] and HM Treasury [294]; for the USA from FinCEN [295] and FATF [274] & [293].

This section compares the AML/CFT systems used in Australia, the UAE, the UK and the USA, based on how these countries comply with the FATF 40+9 Recommendations. It relies upon the published material in the most recent FATF mutual evaluation reports for these countries:

- Australia in 2005 [248]
- UAE in 2007 [261]

\(^{20}\) The UAE AML/CFT system has been evaluated by the IMF, and then the FATF and MENAFATF have adopted the IMF evaluation.
UK in 2006 [273] and 2009 [178]

USA in 2006 [274].

Table 6.2
The FATF core and key recommendations on AML/CFT

<table>
<thead>
<tr>
<th>Recommendation number and its type</th>
<th>Summary of the recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Core</td>
<td>Countries should criminalise money laundering based on the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances</td>
</tr>
<tr>
<td>3 Key</td>
<td>Countries should adopt legal measures to confiscate the proceeds of crime or money laundering</td>
</tr>
<tr>
<td>4 Key</td>
<td>Countries should ensure that privacy laws of financial institutions do not inhibit the implementation of the FATF recommendations</td>
</tr>
<tr>
<td>5 Core</td>
<td>Countries should ensure that financial institutions should have customer due diligence measures for identifying and verifying the identity of their customers</td>
</tr>
<tr>
<td>10 Core</td>
<td>Financial institutions should be required to maintain record keeping for all transactions for at least five years and ensure such information is available to the authorities</td>
</tr>
<tr>
<td>13 &amp; SR IV Core</td>
<td>Financial institutions should be required by law to report suspicious transactions when they suspect or have reasonable ground to suspect that the money is the proceeds of crime, or linked or related to, or will be used for terrorism, terrorism acts or terrorism organisations</td>
</tr>
<tr>
<td>23 Key</td>
<td>Countries should ensure that financial institutions are subject to sufficient regulation and supervision and that they are effectively implementing the FATF recommendations</td>
</tr>
<tr>
<td>26 Key</td>
<td>Countries should establish a financial intelligence Unit (FIU) as a central authority that collects, analyses and distributes information concerning money laundering and the financing of terrorism</td>
</tr>
<tr>
<td>35 &amp; SR I Key</td>
<td>Countries should become a party of, and fully implement the Vienna Convention, the Palermo Convention, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism</td>
</tr>
<tr>
<td>36 Key</td>
<td>Countries should effectively provide mutual legal assistance with regard to AML/CFT investigations, prosecutions and related proceedings</td>
</tr>
<tr>
<td>40 &amp; SR V Key</td>
<td>Countries should ensure that their FIUs provide international cooperation directly with each other to facilitate the exchange of information in relation to AML/CFT</td>
</tr>
<tr>
<td>SR II Core</td>
<td>Countries should criminalise the financing of terrorism, terrorist acts and terrorist organisations</td>
</tr>
<tr>
<td>SR III Key</td>
<td>Countries should have effective laws for the freezing of funds used for terrorist financing</td>
</tr>
</tbody>
</table>

Source: FATF [176, 194]
In the recent FATF evaluation of their AML/CFT systems, the countries were required to submit follow-up reports indicating their progress with achieving compliance. Australia, the UK and the USA have reported back to the FATF. The only published follow-up report arising from these evaluations is one for the UK AML/CFT system that shows that the UK system has made substantial progress and has reached a satisfactory level of compliance with all the core and key recommendations (see Table 6.2) including Recommendation 5, which concerns “customer due diligence and record-keeping”. Follow-up reports for Australia and the USA are not available in the public domain at the time of writing. The UAE has to report to the FATF in March 2010.

Compliance with FATF recommendations is rated as fully compliant (C), largely compliant (LC), partially compliant (PC) and non-compliant (NC). Compliance with each recommendation is measured against essential assessment criteria. This section compares how Australia, the UAE, the UK and the USA comply with the FATF 40 recommendations (see Tables 6.3 and 6.4). The section then proceeds to compare how these four countries comply with the FATF 9 Special recommendations (see Table 6.5).

### 6.1.1 Compliance with the FATF 40 Recommendations

The FATF 40 Recommendations on AML are categorised into four groups, (a) legal systems, (b) preventive measures, (c) institutional and other measures, and (d) international co-operation.

**Legal systems**

From Table 6.3, it is clear that Australia, the UK and the USA are fully or largely compliant with the “Legal systems” Recommendations 1, 2 and 3. The UAE is largely compliant with two recommendations; however, it is partially compliant with Recommendation 1 concerning money laundering offences. The FATF [261] indicated that the UAE has criminalised money laundering, but the predicate offences\(^{21}\) in the law does not cover all the types of serious offences, such as drug

\(^{21}\) According to the UN Convention against corruption, this means any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in Article 23 of this Convention.
trafficking and corruption, that are not completely in accordance with the FATF recommendations.

**Preventive measures**

Australia is non-compliant with nine of the 22 Recommendations, and is only partially compliant with eight other recommendations and, in particular, is non-compliant with the core Recommendation 5 regarding customer due diligence. The FATF [248] noted that customer due diligence is limited in its extent by not covering all the varieties of financial institutions. Australia is only partially compliant with core Recommendation 10 (record keeping) and key Recommendation 23 (financial sector supervision). The FATF indicated that the FTR Act of Australia does not require some cash dealers, such as securities or insurance companies, to keep records of their transactions. The FTR Act was supplemented by the Federal Parliament by the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act). It is anticipated that the AML/CTF Act will rectify many of the shortcomings noted in the previous FATF evaluation report for Australia. Such records are very important for keeping track of all financial transactions. The FATF noted that the AML/CFT (in Australia, they refer to it as the AML/CTF system, instead of AML/CFT) supervisory system is not effective in accordance with its recommendations concerning the system’s need to ensure that the financial institutions have an effective AML/CFT programme in place.

The UAE is non-compliant with seven Recommendations that address “Preventive measures”. The UAE is non-compliant with core Recommendations 5 (customer due diligence) and 13 (suspicious transaction reporting), and is partially compliant with the key Recommendation 23. The FATF noted that there is no core customer due diligence obligations in any law or regulation of the UAE. It added that there are no requirements to implement or undertake ongoing customer due diligence in all financial sectors. With regard to non-compliance with Recommendation 13, the FATF found no requirement in the UAE law or regulations to report suspicious transactions relating to financing of terrorism. The FATF found that there is a lack of a defined basis to recognise a transaction as suspicious. Additionally, the FATF noted that the scope of the AML/CFT
supervisory system and inspection is limited; for instance, there is no supervision of insurance companies. These deficiencies may, in part, be the result of the fact that the UAE law does not impose customer due diligence obligations and does not clarify the UAE’s Financial Intelligence Unit (FIU) responsibilities for the supervision of the financial institutions. These deficiencies have many impacts on the UAE AML/CFT system and result in difficulties in detecting money laundering activities.

The UK is largely or fully compliant with all core and key Recommendations that address “Preventive measures”. However, it is non-compliant with Recommendations 6, 7 and 22 from this group. The FATF [273] indicated that there are no requirements within the UK AML/CFT system concerning the identification of politically exposed persons (PEPs) and noted that there are no requirements specified for financial institutions to collect information concerning correspondent banking.

In addition to being non-compliant with Recommendations 12 and 16, the USA is only partially compliant with Recommendation 5, concerning the establishment of customer due diligence. The FATF [274] found that there are no requirements for some cash dealers, such as life insurance agents, to establish customer due diligence and generally, there are no clear requirements to perform ongoing customer due diligence.

**Institutional and other measures**

With regard to “Institutional and other measures”, Recommendations 26-34, Australia is partially compliant with Recommendations 29 and 34. The FATF noted that the AUSTRAC powers of enforcement are limited to criminal sanctions and appear to be rarely applied. The FATF also indicated that authorities have the power to access information concerning beneficial ownership, but the system is inadequate. While the AML/CFT system of Australia has some problems in compliance with the previous recommendations, it is fully compliant with key Recommendation 26. In contrast, the UAE system is partially compliant with Recommendation 26 concerning the FIU.
### Table 6.3

Comparison of compliance with the FATF 40 recommendations between the AML systems used in Australia, the UAE, the UK and the USA

<table>
<thead>
<tr>
<th>Recommendations</th>
<th>Type</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legal systems</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Core</td>
<td>LC</td>
<td>PC</td>
<td>C</td>
<td>LC</td>
</tr>
<tr>
<td>2</td>
<td>LC</td>
<td>LC</td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Key</td>
<td>C</td>
<td>LC</td>
<td>C</td>
<td>LC</td>
</tr>
<tr>
<td>4</td>
<td>Key</td>
<td>C</td>
<td>LC</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>5</td>
<td>Core</td>
<td>NC</td>
<td>NC</td>
<td>LC</td>
<td>PC</td>
</tr>
<tr>
<td>6</td>
<td>NC</td>
<td>NC</td>
<td>NC</td>
<td>LC</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>NC</td>
<td>NC</td>
<td>NC</td>
<td>LC</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>NC</td>
<td>LC</td>
<td>C</td>
<td>LC</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>NC</td>
<td>LC</td>
<td>PC</td>
<td>LC</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Core</td>
<td>PC</td>
<td>LC</td>
<td>C</td>
<td>LC</td>
</tr>
<tr>
<td>11</td>
<td>PC</td>
<td>LC</td>
<td>PC</td>
<td>LC</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>NC</td>
<td>NC</td>
<td>PC</td>
<td>NC</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Core</td>
<td>LC</td>
<td>NC</td>
<td>C</td>
<td>LC</td>
</tr>
<tr>
<td>14</td>
<td>C</td>
<td>PC</td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>NC</td>
<td>PC</td>
<td>LC</td>
<td>LC</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>NC</td>
<td>NC</td>
<td>LC</td>
<td>NC</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>PC</td>
<td>PC</td>
<td>LC</td>
<td>LC</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>PC</td>
<td>PC</td>
<td>PC</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>C</td>
<td>PC</td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>PC</td>
<td>PC</td>
<td>PC</td>
<td>LC</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>NC</td>
<td>LC</td>
<td>NC</td>
<td>LC</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Key</td>
<td>PC</td>
<td>PC</td>
<td>LC</td>
<td>LC</td>
</tr>
<tr>
<td>24</td>
<td>PC</td>
<td>NC</td>
<td>PC</td>
<td>PC</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>PC</td>
<td>PC</td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Key</td>
<td>C</td>
<td>PC</td>
<td>LC</td>
<td>LC</td>
</tr>
<tr>
<td>27</td>
<td>LC</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>28</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>29</td>
<td>PC</td>
<td>PC</td>
<td>LC</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>30</td>
<td>LC</td>
<td>PC</td>
<td>LC</td>
<td>LC</td>
<td>C</td>
</tr>
<tr>
<td>31</td>
<td>LC</td>
<td>LC</td>
<td>C</td>
<td>LC</td>
<td>C</td>
</tr>
<tr>
<td>32</td>
<td>LC</td>
<td>PC</td>
<td>LC</td>
<td>LC</td>
<td>LC</td>
</tr>
<tr>
<td>33</td>
<td>LC</td>
<td>PC</td>
<td>PC</td>
<td>NC</td>
<td>LC</td>
</tr>
<tr>
<td>34</td>
<td>PC</td>
<td>PC</td>
<td>C</td>
<td>PC</td>
<td>LC</td>
</tr>
<tr>
<td>35</td>
<td>Key</td>
<td>LC</td>
<td>C</td>
<td>C</td>
<td>LC</td>
</tr>
<tr>
<td>36</td>
<td>Key</td>
<td>C</td>
<td>LC</td>
<td>LC</td>
<td>LC</td>
</tr>
<tr>
<td>37</td>
<td>C</td>
<td>LC</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>38</td>
<td>C</td>
<td>PC</td>
<td>C</td>
<td>LC</td>
<td>LC</td>
</tr>
<tr>
<td>39</td>
<td>C</td>
<td>LC</td>
<td>C</td>
<td>LC</td>
<td>LC</td>
</tr>
<tr>
<td>40</td>
<td>Key</td>
<td>C</td>
<td>PC</td>
<td>C</td>
<td>C</td>
</tr>
</tbody>
</table>

Notes: C: fully compliant; LC: largely compliant; PC: partially compliant; NC: non-compliant.

The FATF found that the UAE's FIU has some problems in relation to collecting, analysing and disseminating suspicious activity reports. The FATF also noted that the FIU of the UAE does not publish annual reports with statistics concerning its
activities. It is difficult to find information on the number of suspicious transactions reported each year in the UAE, as we found in a separate work [296]. This information, if it is collected and analysed appears not to be published generally.

The UK AML/CFT system is partially compliant with Recommendations 33 and 34. The FATF noted that the UK system does not have sufficient measures to identify accurate information concerning beneficial ownership. The USA AML/CFT system has some problems in compliance with Recommendations 33 and 34. The FATF indicated that the USA system does not have adequate measures in place to ensure that there is accurate information available on beneficial ownership.

*International co-operation*

With regard to Recommendations 35–40, Australia, the UK and the USA are fully or largely compliant with these Recommendations. In contrast, the UAE is less compliant than the other countries. It is partially compliant with Recommendations 38 and key Recommendation 40. It is expected that the UAE will address these areas of deficiencies. The main deficiency is that there are no legal provisions that define how confidential information will be shared with other foreign counterparts.

As shown in Table 6.4, the USA followed by the UK appearing to be the most advanced in terms of compliance, with the UAE being the least compliant.

**Table 6.4**

Summary of compliance with the FATF 40 Recommendations on AML

<table>
<thead>
<tr>
<th>Country</th>
<th>Fully compliant (C)</th>
<th>Largely compliant (LC)</th>
<th>Total (C+LC)</th>
<th>Partially compliant (PC)</th>
<th>Non compliant (NC)</th>
<th>Total (PC+NC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>12</td>
<td>9</td>
<td>21</td>
<td>10</td>
<td>9</td>
<td>19</td>
</tr>
<tr>
<td>UAE</td>
<td>5</td>
<td>12</td>
<td>17</td>
<td>16</td>
<td>7</td>
<td>23</td>
</tr>
<tr>
<td>UK</td>
<td>19</td>
<td>10</td>
<td>29</td>
<td>8</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td>USA</td>
<td>12</td>
<td>22</td>
<td>34</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
</tbody>
</table>
6.1.2 Compliant with the FATF 9 Special Recommendations

This section compares the compliance with the FATF 9 special recommendations on Combating Financing of Terrorism (CFT). The FATF simultaneously evaluated the CFT and AML systems in Australia, the UAE, the UK and the USA. Table 6.5 illustrates a summary by countries of the compliance with the FATF 9 special recommendations on CFT. Once again, the USA, followed by the UK appears to be the most advanced in terms of compliance, with the UAE being least compliant.

Australia, the UK and the USA are either compliant or largely compliant with the core and key Special Recommendations. In contrast, the UAE is non-compliant with core Special Recommendation IV concerning suspicious transaction reporting. The UAE is only partially compliant with the key Special Recommendation I regarding implementing the 1999 UN International Convention for the Suppression of the Financing of Terrorism, and the key Special Recommendation III regarding imposing effective laws for freezing and confiscation of funds used for financing of terrorism.

Table 6.5
Summary of compliance with the FATF 9 special recommendations on CFT

<table>
<thead>
<tr>
<th>Country</th>
<th>Fully compliant (C)</th>
<th>Largely compliant (LC)</th>
<th>Total (C+LC)</th>
<th>Partially compliant (PC)</th>
<th>Non compliant (NC)</th>
<th>Total (PC+NC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>-</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>UAE</td>
<td>-</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>UK</td>
<td>5</td>
<td>3</td>
<td>8</td>
<td>1</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>USA</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

6.1.3 Implications of Non-compliance with FATF

Overall, Australia is non-compliant or partially compliant with three core and key Recommendations (5, 10 and 23). The UAE is non-compliant or partially compliant with nine core and key Recommendations (1, 5, 13, 23, 26, 40, SR I, SR III and SR IV). The USA is only partially compliant with core Recommendation 5. This finding suggests that there are additional steps that need to be taken by Australia, the UAE and the USA to address the identified deficiencies. The UAE, in particular, needs to
do more work to ensure that its AML/CFT system is effectively implemented in accordance with the FATF recommendations.

Non-compliance with the FATF recommendations has negative implications for a country and its relations with other countries. A country’s non-compliance with the FATF recommendations implies corresponding risks of unfettered money laundering and the financing of terrorism. The implications of non-compliance include the increased risk of exploiting a country’s financial system for criminal purposes by organised criminals and terrorists, with implications for a country’s economy, society and victims of crime [52]. The New Zealand Government notes [297], “[t]he overall objective of implementing these standards [FATF Recommendations] is to reduce crime in New Zealand and therefore to make New Zealand communities safer … the national interest requires that New Zealand complies with all FATF Recommendations”.

But what are the implications of a country’s non-compliance with the FATF recommendations for its relationship with other jurisdictions? The New Zealand Government also notes [297] that it can impact on a country’s international reputation in the following ways [297]:

- Increased costs of borrowing from abroad, because overseas lenders may recognise the country as being a greater financial risk.
- A non-compliant country may have difficulties in trading with other countries and its companies will have also some difficulties in doing business overseas.
- Relations with international organisations, such as the World Bank and the IMF, could be affected.
- The country may be seen as a haven or place for money launderers and terrorism financiers.

There are specific implications for non-compliance when dealing with countries that are compliant. To protect its interests and minimise risk, a compliant country may impose tough regulations in dealing with non-compliant countries. A non-compliant country could face many obstacles from international organisations and other compliant countries, such as discouraging foreign investment, trade and relationships, and its reputation with international
organisations, such as the World Bank and the IMF, would be affected. The IMF (2009) [298] noted the following:

Money laundering and terrorist financing activities can undermine the integrity and stability of financial institutions and systems, discourage foreign investment, and distort international capital flows. In an increasingly interconnected world, the problems presented by these activities are global, as are the links between financial stability and financial integrity. Money launderers exploit differences between national anti-money laundering laws and systems, especially in jurisdictions with weak or ineffective controls where they can move their funds more easily. Moreover, problems in one country can quickly spread to other countries in the region or in other parts of the world.

There are other implications too. For instance, a non-compliant country may not be able to provide useful or helpful information, such as customer identification and financial transactions records, to assist in tracing the origins of transaction monies. Such problems are especially serious in the modern context of globalization, because money laundering and the financing of terrorism are global problems that take place across multiple jurisdictions and need to be combated at both the national and international levels.

A well-developed and implemented AML/CFT system can improve a country's ability to combat money laundering and the financing of terrorism and therefore, improve the integrity and stability of its financial system. In fact, an effective AML/CFT system in place protects a country's interests and reputation in terms of its relationships with other countries. In 2009, the G20 Working Group on Reinforcing International Cooperation and Promoting Integrity in Financial Markets [299] indicated that countries should implement measures that protect the global financial system from uncooperative or non-compliant countries by using FATF recommendations that create risks for illicit financial systems. This clearly shows the negative internal and external implications on a non-compliant country with the FATF recommendations.
In conclusion, the non-compliance with the FATF Recommendations means a heightened risk for a country’s financial systems, reputation and its interests in dealing with other countries in an extremely globalised world.

### 6.2 Discussion: Factors Affecting Compliance

The previous section analysed and compared the extent of the compliance of the four countries with the FATF recommendations. We found that the UAE is the least compliant with the Recommendations. There are various fundamental factors that are expected to be important in determining how a country such as the UAE develops and implements its financial and AML/CFT systems. This section examines some of the factors that have arguably affected the UAE’s compliance, in particular, the religious and cultural, and socio-economic and financial factors that appear to be important. Also, Chapter 5 has indicated briefly to the results of the analysis in this section.

#### 6.2.1 Religious and Cultural Factors

The UAE’s culture has developed from a strong belief in Islam, which governs the people's way of life, behaviour and decisions [300]. This has had a significant impact on the UAE culture. The UAE culture is, accordingly, in many ways significantly different from the culture in Australia, the UK and the USA.

The founding members of the FATF – which did not include the UAE – such as Australia, the UK and the USA, have unavoidably left their cultural imprints on the organisation and its operations. This has some natural consequences when it comes to FATF evaluations. Johnston and Carrington (2006) [301] indicate that there is a problem when the FATF institutes a mutual assessment evaluation of the AML/CFT systems in member countries. This problem is how to implement the FATF standards that have been structured in the context of developed countries and apply them to the financial markets of developing countries [301], countries, typically, with a different culture and history. Johnston and Carrington note that trying to impose measures that are unsuitable for developing countries, may lead to the non-compliance with the FATF standards [301].

Kanatas and Stefanidis [290] note that culture and legal systems support each other and that economic development and financial structures are affected not
only by a country’s legal system, but also by its culture and show that the development of a country’s legal and financial systems are related to its religious beliefs. They note that culture is “the engine of economic prosperity and growth and a critical factor in the development of financial markets”. When people talk about culture, they talk about a way of life, what people believe and how they apply that to develop their regulations, organisations and institutions. Kwok and Tadesse (2005) [302] argue that countries differ in the configuration of their financial systems, because they are different in their national cultures.

According to the USA Department of State (2007), Islam is practiced by 96% of the population in the UAE [303], making it a dominant influence in the country. Islam prohibits any activity funded by money derived from unlawful trade or ill-gotten property and prohibits using illegal money for charities [289]. Money gained from gambling and bank interest is prohibited in Islam [289]. This is in marked contrast to the normal practice in Australia, the UK and the USA. Torgler (2006) [304] noted that “[r]eligious guidance measures the obligation to follow particular rules that define what is good and evil”. The individual’s behaviour is associated with what they believe. For instance, Torgler (2006) [304] found a strong connection between religiosity and tax compliance. Rowan Bosworth-Davies [305] indicated the following:

_Influenced in America, by strong, fundamentalist Bible-Belt dogma, or the arcane language of the new puritan religious agendas which have increasingly made themselves apparent in the UK, much of the debate which underpins the agenda on financial crime and money laundering is … discussed in the language of a conventional but aggressive Judeo/Christian morality._

While there is no income tax in the UAE, Muslims are required, as a part of their religion, to “[fulfill] the God right through paying money – ‘Zakat’ – to charities or to the needy people”. [289] Charities play an important role in Muslim practices. Crimm (2008) [306] noted that:

_As Islam places a high value on compassion, wealth redistributions, social justice, and supporting and enhancing fellow humans, both philanthropy and charity play crucial roles for Muslims and their civil societies._ The
flow of such funds is economically essential to, and provides critical building blocks for, Muslim civil societies.

The FATF Special Recommendation VIII indicates that countries should have effective laws and regulations concerning non-profit organisations that can be misused for the financing of terrorism, including taking a risk-based approach that identifies the aims of the organisation, its size and the amount of money it handles [176, 307]. The problem is in identifying what kind of activities constitutes terrorism and whether financing such activities would be considered as financing terrorism. The World Bank (2006) [308] noted that while countries have agreed on combating financing of terrorism, the “meaning of terrorism is not universally accepted due to significant political, religious and national implications that differ from country to country”.

Crimm [306] indicated that implementing the FATF strict standards on AML/CFT could affect the extent of the Muslim charities and consequently effectively “cut off” financial support for the needy. Many countries, such as the UAE, have imposed some obligations on charitable organisations to protect them from misuse. All charitable organisations in the UAE are regulated and monitored by the Ministry of Social Affairs [291]. The UAE also specifies legitimate channels for charities to transfer money outside the country to minimise the possible use of these funds for illegal purposes. In 2002, the UAE Government regulated that all licensed charitable organisations wishing to transfer money overseas, must do so through either, the Red Crescent Authority, the Zayed Charitable Foundation or the Muhammad Bin Rashid Charitable Trust [291]. This allows people to make charitable donations whose destinations can be monitored.

According to the IMF [309], Islamic banking is characterised as follows:

Activities of Islamic financial institutions differ from those of standard commercial depository corporations in that predetermined interest on financial transactions is prohibited. The nonpayment of interest on liabilities does not in itself preclude instruments from being classified as external debt.
Islam’s prohibition on bank interest means that an important service provided by Islamic banking is the buying and selling of goods without interest. For example, if a person wants to buy a car, they do not give the money directly to the seller. Instead, the bank buys the car and resells it to the buyer and customer. This practice is called Murabaha [310] and is pervasive throughout the UAE Islamic banking sector. The HSBC Amanah (2009) [310] defines Murabaha as (the):

... purchase and resale. Instead of lending out money, the capital provider purchases the desired commodity (for which the loan would have been taken out) from a third party and resells it at a predetermined higher price to the capital user. By paying this higher price over installments, the capital user has effectively obtained credit without paying interest.

We note that some non-Islamic banks in Australia, for instance, have started to recognise the need for such services; this is, again, in marked contrast to the normal practice in Australia, the UK and the USA.

As mentioned in Chapter 5, the UAE is a cash-based economy in which carrying large cash amounts is a normal practice; this makes it more difficult to impose requirements concerning the reporting of large cash transactions. Imposing regulations (for instance, requiring all large transactions to be reported) in such circumstances is very difficult, if not impossible. While many consider this to be a good cultural trait, it is problematic for the purpose of analysing the cycle of money. Finally, the UAE is a society with a strong homogeneity [287] that is characterised by strong, extended, family relationships and close family ties [311]. There is a concern here, especially when applying the FATF standards concerning customer due diligence. For instance, if a person goes to a bank to conduct a transaction and finds that he/she knows the bank’s employee, it is quite likely that the employee will not undertake due diligence procedures. In fact, this practice is not limited only to the UAE culture, although it is considerably more prevalent in the UAE than the other countries. Bedi and Acharya [312] note that personal relationships “can lead to poor compliance [with AML] standards as many USA Private Banks have found out”.

In the UAE, carrying large sums of cash and purchasing properties and expensive products for cash is normal [261]. The USA Department of State [291]
6.2 Discussion: Factors Affecting Compliance

noted that according to the UAE, “[c]ustoms officials, police, and judicial authorities tend to not regard large cash imports as potentially suspicious or criminal type activities, arguing that the UAE is a cash-based economy, and it is not unusual for people to carry significant sums of cash”.

6.2.2 Socio-economic and Financial Factors

For the purpose of this section, it is worthwhile to examine the population and the size of the GDP in Australia, the UAE, the UK and the USA. Table 6.6 illustrates the population and the GDP for these four countries from 1999 to 2008.

Table 6.6 shows clearly that there is a significant difference between the population and the size of the GDP in the UAE, compared to those in Australia, the UK and the USA.

The USA Department of State (2007) indicates that oil makes up most of the UAE export earnings thus dominating the economy [303]. Also, according to Australia’s Department of Foreign Affairs and Trade (2008) [313], “the UAE has the world’s third largest conventional oil reserves and fifth largest natural gas reserves and is a major player in world energy markets ...”. Oil provides wealth to the country and its people.

One of the socio-economic factors that affects the UAE financial system and differentiates it from the other three countries is the use of the Hawala system. As indicated in Chapter 5, the Hawala system is used to transfer money or value between people in a local community without any interaction with financial institutions. Viles (2008) [314] defines Hawala as “a system by which people in geographically remote areas can give things of value to each other, without the physical (and, now, without the electronic) conveyance of money”. The UAE has established regulations in relation to Hawala that require that Hawaladars should register themselves and then become recognised as Hawala Brokers [288]. The UAE intend to ensure that the Hawala brokers provide details of money transfers and report any suspicious transfers. The registration is still voluntary and UAE authorities have no legal power to examine Hawaladars for non-compliance.
Table 6.6
The population and GDP of Australia, UAE, the UK and the USA, 1999–2008

<table>
<thead>
<tr>
<th>Year</th>
<th>Australia Population (millions)</th>
<th>UAE GDP in billions US$</th>
<th>UAE Population (millions)</th>
<th>UK GDP in billions US$</th>
<th>UK Population (millions)</th>
<th>USA GDP in billions US$</th>
<th>USA Population (millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1999</td>
<td>18.957</td>
<td>401.998</td>
<td>3.033</td>
<td>55.181</td>
<td>58.684</td>
<td>1,502.89</td>
<td>279.195</td>
</tr>
<tr>
<td>2000</td>
<td>19.187</td>
<td>389.956</td>
<td>2.995</td>
<td>70.221</td>
<td>58.886</td>
<td>1,480.53</td>
<td>282.291</td>
</tr>
<tr>
<td>2001</td>
<td>19.445</td>
<td>368.123</td>
<td>3.167</td>
<td>68.677</td>
<td>59.113</td>
<td>1,471.40</td>
<td>285.177</td>
</tr>
<tr>
<td>2002</td>
<td>19.684</td>
<td>412.914</td>
<td>3.349</td>
<td>75.892</td>
<td>59.323</td>
<td>1,614.70</td>
<td>287.943</td>
</tr>
<tr>
<td>2003</td>
<td>19.927</td>
<td>527.760</td>
<td>3.551</td>
<td>88.959</td>
<td>59.557</td>
<td>1,862.77</td>
<td>290.619</td>
</tr>
<tr>
<td>2004</td>
<td>20.163</td>
<td>640.573</td>
<td>3.761</td>
<td>107.304</td>
<td>59.846</td>
<td>2,199.25</td>
<td>293.236</td>
</tr>
<tr>
<td>2005</td>
<td>20.437</td>
<td>713.262</td>
<td>4.106</td>
<td>135.198</td>
<td>60.238</td>
<td>2,280.06</td>
<td>295.924</td>
</tr>
<tr>
<td>2006</td>
<td>20.740</td>
<td>755.21</td>
<td>4.229</td>
<td>164.165</td>
<td>60.587</td>
<td>2,335.70</td>
<td>298.700</td>
</tr>
<tr>
<td>2007</td>
<td>21.059</td>
<td>909.743</td>
<td>4.488</td>
<td>180.18</td>
<td>60.890</td>
<td>2,803.40</td>
<td>301.617</td>
</tr>
<tr>
<td>2008</td>
<td>21.323</td>
<td>1,010.70</td>
<td>4.764</td>
<td>260.141</td>
<td>61.073</td>
<td>2,674.09</td>
<td>304.415</td>
</tr>
</tbody>
</table>

Source: The IMF [109], World Economic Outlook Database, April 2009.

Australia, the UK and the USA are all recognised as developed countries, while the UAE is a developing country. In the UAE, in contrast to Australia, the UK and the USA, there is no tax on income and this has at least two interesting implications. The first is that the motivation for money laundering to achieve tax avoidance is absent. The second is that the cycle of money is harder to trace, as a result of not having to report income. The obligatory reporting of income in other countries enables the flow of money to be more easily followed. While the UAE requires financial institutions to report any transactions that are unusually large for a given account with no legal purpose or reasonable or economic grounds [190], there is no general requirement to report income by companies or by individuals.

The financial systems in Australia, the UK and the USA are very similar and are dominated by their stock markets [302] and although UAE financial systems have some similarities with these countries, there are important differences as indicated above. These differences play an important role in how the country implements its AML/CFT system.
6.2.3 Summary

While one might conjecture that the differences in the AML/CFT systems simply reflect a specific country’s needs and situation and may, therefore, be entirely appropriate in a local sense, the fact is that money laundering is a global problem and individual cases very often involve international transactions. This, in turn, makes it inevitable that a high degree of international harmonisation is paramount. This presents a problem for the international community and the FATF that can be solved only by a careful, country-by-country, consideration of the local factors. Overall, we believe that further steps are needed by both the UAE and the FATF to enable a shift in the UAE culture that facilitates compliance.

6.3 Conclusion

This chapter investigated the implementation of the FATF Recommendations by the international community. It discussed the AML/CFT systems of Australia, the UAE, the UK and the USA. It also reviewed the history and the nature of the FATF, and how it assesses and evaluates the AML/CFT systems of the member countries. The chapter found that there are some gaps, and the FATF member countries need to do more work to remain faithful to its standards.

The chapter found that Australia, the UAE and the USA have some problems with compliance with the FATF 40+9 Recommendations. These countries are partially compliant or non-compliant with some of the core and key Recommendations. The UAE is non-compliant or partially compliant with nine core and key Recommendations. Australia is non-compliant or partially compliant with three core and key Recommendations. USA is non-compliant or partially compliant with core Recommendation 5.

This finding also suggests that there are additional steps that need to be taken by Australia, the UAE and the USA to address the identified deficiencies and other areas that need to be strengthened. Overall, both the UK and the USA have the best AML/CFT systems among these four countries based on their compliance with the FATF recommendations. The AML/CFT systems used in Australia and the UAE need more work to be compliant with the FATF 40+9 Recommendations. The AML/CFT system of the UAE, in particular, is less compliant with these
recommendations. This chapter suggests that some local factors have influenced the implementation of the FATF Recommendations, which factors include religious and cultural, socio-economic and financial. These factors represent a real challenge to any country such as the UAE when implementing its regulations and financial institutions and, given the global and widespread nature of money laundering, it is vital that local and international communities cooperate to meet the recommendations. In conclusion, this chapter attempts to understand better how different countries comply with the FATF standards and how the AML/CFT systems in these countries are affected by local factors.

Chapter 7 summarises the whole research project and discusses the implications of it for further research.
Chapter 7
Conclusion and Future Work

The objective of this thesis was to examine the extent to which there is a common and effective approach for combating computer crime internationally and the extent to which such efforts are succeeding and what improvements are needed. It was aiming to investigate and compare different jurisdictions from around the world and their approaches to combating computer crime with a view to understanding the effectiveness of their approaches and the factors that have influenced that.

This thesis examined the approaches used for combating computer crime in Australia, the UAE, the UK and the USA, four countries which represent a spectrum of economic development and culture. In the case of the UAE, we also examined the cultural influences that differentiate it from the other three countries and which have necessarily been a factor in shaping its approaches for countering money laundering in particular, an especially insidious and significant form of computer crime. We have selected these four countries for a number of reasons. The UAE has been selected because the funding for this research has been provided by the UAE and because the UAE, while a modern and fast developing economy, is an Islamic jurisdiction and thus, to that extent, distinctly different from the other three countries. Australia is included because the research has been undertaken in Australia. The UK has been selected as a jurisdiction representative of the European Community, and the USA has been selected for a number of reasons, the main one being that, as the world’s largest economy, it needs to be included in any study of this nature.

This chapter is a summary of the main contributions and achievements of this thesis and presents possible future directions for related research.
7.1 Summary of Contributions

The thesis concludes that because of the transnational nature of computer crime or cybercrime there is a need internationally for further harmonisation of approaches for combating computer crime. The principal contributions and achievements of this thesis are as follows:

- Proposing a unified comprehensive taxonomy of computer crime which identifies how computer crimes may be classified based upon the dual characteristics of the role of the computer and the contextual nature of the crime
- Revealing similarities and differences in computer crime legislation in Australia, the UAE, the UK and the USA, and how they correspond to the CoE Convention on Cybercrime and proposing a new framework to develop harmonised computer crime or cybercrime legislation globally
- Revealing that there are some important issues that continue to create problems for law enforcement agencies such as sufficient resources and coping internationally with computer crime legislation that differs between countries. This thesis also highlights the importance of having comprehensive documented procedures and guidelines for combating computer crime, and reporting and recording of computer crime offences as distinct from other forms of crime
- Presenting the most comprehensive study currently available regarding the extent of money laundered in four such developed or fast developing countries
- Identifying that the UK and the USA are the most advanced with regard to anti-money laundering and combating the financing of terrorism (AML/CFT) systems among the four countries based on compliance with the FATF recommendations. In addition, identifying that Australia and the UAE have further to go to be compliant with the FATF recommendations, and the UAE in particular is least compliant with these recommendations among the four studied countries. The thesis identified that local factors have affected how the UAE has implemented its financial and AML/CFT systems and that such local and cultural factors should be taken into account when implementing or evaluating any country’s AML/CFT system.
7.2 Future Work

This section proposes a number of potential future research directions based on the work presented in this thesis.

**Extent of alignment with the CoE Convention on Cybercrime of other countries**

Chapter 3 identified that Australia, the UAE, the UK and the USA have legislation that covers offences related to computers and computer systems. It also provided a preliminary analysis of the extent to which that legislation in these four countries is in alignment with the Articles 2 to 11 of the CoE Convention. An important next step especially in view of the recent failure at the UN to establish a global cybercrime treaty would be to identify to what extent the UAE would compare to other Middle Eastern countries such as Saudi Arabia and Jordan in relation to their alignment with the CoE Convention. Furthermore, it would be more useful to include the detailed evaluation of conformance of cybercrime legislation of many countries, from different regions and cultures, and investigate to what extent they correspond to the CoE Convention. This is outside the scope of this thesis but it does warrant further investigation.

**Harmonisation of computer crime legislation**

Chapter 3 proposed a framework to develop harmonised computer crime or cybercrime legislation at the global level. Clearly, given UN efforts in this regard, this is an important objective. Our proposed framework builds upon ideas from and takes advantage of the relative success of the FATF moves towards establishing a global approach to AML/CTF legislation and governance. Overall, more detailed analysis of the feasibility of implementation of the proposed five stage framework is needed. This future research should consider the local factors of each country or region as there are many factors, such as cultural and economic factors, affecting how countries develop and implement their regulations and legislation. It also worthwhile to investigate to what extent harmonisation of legislation would resolve at least some existing problems relating to extradition.
Law Enforcement Agencies and the Reporting of Cybercrime

Chapter 4 investigated and identified the differences and similarities in their approaches to combating cybercrime of two different law enforcement organisations, the QPS from Australia and ADP from the UAE, as a case study with implications in the more general international context. In fact, Chapter 4 indicated to the need for better approaches for combating computer crime. A future work could build from this work and undertake a comprehensive and detailed study of law enforcement agencies – for instance, all state law enforcement agencies in Australia and likewise in the UAE, accompanied also by possibly the British Police and the FBI from the USA. Additionally, there is a need for a future research into the existence of comprehensive reporting of computer crime at the national level in order to provide regulators and legislators with accurate information on computer crime trends. The reporting needs to include data regarding all cases, regardless of courtroom outcome, together with the extent of resources involved.

Money laundering and FATF compliance

Chapter 6 found that Australia, the UAE and the USA have some problems with compliance with the FATF 40+9 Recommendations. These countries are partially compliant or non-compliant with some of the core and key Recommendations. These countries were required to submit follow-up reports indicating their progress with achieving compliance. Therefore, an ongoing research into how the level of FATF compliance by Australia, the UAE and the USA has changed is very important. Additionally, this ongoing research should consider many other countries to identify their level of compliance. This is outside the scope of this thesis, but worthwhile further research.

7.3 Conclusion

The global nature of the Internet has resulted in enormously increased opportunities for the cyber criminals. Computer crime or cybercrime is increasingly becoming one of the main threats to the well being of the nations of the world. Therefore, it is clear that there is a crucial need for a common understanding of such criminal activity internationally to deal with it effectively. It is likewise very important to explore and understand the problem in detail and to
identify obstacles to international cooperation in combating computer crime. It is also important to identify and adopt best approaches for combating computer crime. This requires continued research into the extent to which legislation, international initiatives, policy and procedures, and technology to combat and investigate computer crime are consistent globally and can be improved upon.

In conclusion, our work have identified and proposed some of the important aspects in combating computer crime and harmonisation of legislation. Besides that, it promotes for further research directions in order to combat computer crime more effectively.
Bibliography


125. Broersma, M. *Police Turn to IT Industry to Help Fight Cybercrime*. 2009 [cited 2010 19 May]; Available from:


171. FATF. History of the FATF. [cited 2009 4 April]; Available from: http://www.fatf-gafi.org/document/63/0,3343,en_32250379_32236836_34432255_1_1_1_1_1_00.html.

172. FATF. Members & Observers. [cited 2010 27 January]; Available from: http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236869_1_1_1_1_1_1,00.html.


174. FATF. Mutual Evaluations Programme. [cited 2009 15 April]; Available from: http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236982_1_1_1_1_1_1,00.html.


media/conferences/gambling00/mcmillen.ashx.

Press. 546.

technologies as tools to investigate money laundering*. Police Practice and

187. Zdanowicz, J., *Detecting Money Laundering and Terrorist Financing via Data

188. AUSTRAAC. *Timeline*. 2009 5 Feb 2009 [cited 2009 24 April]; Available from:


190. UAE Government. *Laws, Regulations and Procedures Implemented in the UAE
for Anti-Money Laundering and Combating Terrorism Financing*. 2005


193. Comptroller of the Currency Administrator of National Banks/ U.S.
Department of the Treasury. *Bank Secrecy Act/Anti-Money Laundering.*
2000 [cited 2009 13 December]; Available from:

194. FATF. *The 40 Recommendations*. 2003 2004 [cited 2009 1 August];
Available from: http://www.fatf-gafi.org/dataoecd/7/40/34849567.PDF.

195. USA Code of Federal Regulations. *USA Code of Federal Regulations - Title 12:
Banks and Banking: Part 21—Minimum security devices and procedures,
reports of suspicious activities, and Bank Secrecy Act compliance program.*
[cited 2009 12 December]; Available from:
http://ecfr.gpoaccess.gov/cgi/t/text/text-
idx?c=ecfr&sid=7d3cf311cf2afca551913296aa8c2200&rgn=div5&view=tex
r&node=12:1.0.1.1.19&idno=12.

196. Kornakov, K. *Changes to UK Cybercrime Legislation are in the Air*. 2007
[cited 2008 3 January]; Available from:


198. Smith, R.G., *Impediments to the successful investigation of transnational high
tech crime*. 2004, Australian Institute of Criminology.

23-32.


Bibliography


247. FATF. *Money Laundering FAQ.* 2009 [cited 2009 7 August]; Available from: http://www.fatf-


Appendices

Appendix A: Detailed Analysis of Computer Crime Case Studies

Appendix A presents our detailed analysis of the following computer crime case studies:

- Morris worm [226]
- Maroochydore public waterways sewage [227]
- Harassment letter send by email
- USA v. Gorshkov & USA v. Ivanov [228, 229]
- Fungible credentials [230]
- International Interpol-led investigation on child pornography [231]
- ShadowCrew [232]
- Holiday prize scam [233]
- Fraud and money laundering scheme [234].

**Morris worm**

In 1988, *Morris* wrote a program that aimed to measure the size of the Internet, according to its creator [226]. However, this worm copied itself from one computer to another and caused a lot of disruption to numerous networks and computer systems. Through exploiting known vulnerabilities, the worm could infect each computer several times in order to slow it down to make it unusable. *Morris* noted that his program had been designed to hide in the network; nevertheless, because of a single inaccuracy, it multiplied very quickly disrupting many computer networks [226]. The spreading mechanism in the worm resulted in creating a denial of service (DoS) attack. In 1990, a Federal USA judge placed *Morris* on three years’s probation, fined him by US$10,000 and ordered him to perform 400 hours of community service for intentionally disrupting nationwide computer networks [226].

**Maroochydore public waterways sewage**

In 2000, *Vitek Boden* used a stolen computer and radio transmitter to pump thousands of litres of raw sewage into public waterways in Maroochydore
Boden was a former employee at Hunter Watertech. At that time, Hunter Watertech was the supplier of Maroochydore Shire’s remote control and telemetry. Boden’s aim from the pollution he caused was trying to obtain a consulting job with the shire council to clean up what he was causing. After two months, in April 2000, the Boden pollution was discovered and subsequently, the Court found him guilty of 30 charges of computer hacking. Boden’s pollution caused serious environmental harm to the Maroochydore public waterways [227].

**Harassment letter send by email**

A person X typed a harassment or threat letter in his computer and then sent it using his email account to person Y. The victim, who received the email, printed the email and reported the case to the police. Later on, the person X denied his relationship to the email. After seizing his computer, the investigators found a digital copy of the letter that indicated the connection of person X to the offence.

**USA v. Gorshkov & USA v. Ivanov**

In 1999, the FBI received a complaint from Speakeasy, an Internet Services Provider that its network has been compromised and some of its systems were under computer attack [229]. Speakeasy mentioned that personnel credit card details had been stolen and the attacker had sent an email to the company asking to be hired as a security reviewer for the company’s network. The attacker threatened the company but it refused to respond to his demands. Some other similar series of attacks such as DoS attacks took place at other online sites such as Online Information Bureau of Vernon (OIB) and CNN website [229]. Alexey Ivanov had also introduced himself to OIB seeking a job. The FBI were called him and identified that Ivanov’s location was in Chelyabinsk, in Russia, and they identified that he was involved in a business website called ‘tech.net.ru’ [229]. The FBI planned a sting operation to bring Ivanov to the USA where he could be arrested. One FBI agent made telephone contact with Ivanov, however, the person who answered the call was Vasily Gorshkov. Then, both Ivanov and Gorshkov were invited to interview for a job in a fake company in the USA and to demonstrate their skills. In 2000, they went to the USA and completed the interview, and
immediately after that, the FBI arrested them [228, 229]. Ivanov and Gorshkov have been charged with conspiracy, computer hacking, computer extortion, wire fraud, and obtaining information without authorisation and causing damage to computers [228, 229].

**Fungible credentials**

One example of fungible credentials is a driver’s license that has been issued to an individual under a fabricated or false name or information. The counterfeit driver's license is created mostly for criminal purposes such as identity theft, financial fraud and money laundering [230]. In fact, criminals use the computer as a tool to counterfeit legitimate documents such as driver's licenses using a range of machines from simple printers to sophisticated replicating machines [230].

**International Interpol-led investigation on child pornography**

In 2008, a hacker posted 99 child pornography images on a private European-based website and in just 76 hours, there were 12 million hits to the website from 150,000 computer users [231]. Because the investigation involves 170 countries, Interpol led the investigation. There were thousands of people identified and under investigation from around the world, including 1,500 individual computers in Australia [231].

**ShadowCrew**

Mantovani was a member of different cyber groups that generally dealt in storing stolen information and documents [232]. Afterward, he thought about an online place to sell off stolen goods and share hacking tricks. In 2002, Andrew Mantovani and David Appleyard started running ‘shadowcrew.com’ as an international clearinghouse for stolen credit cards, identity information, DDoS attacks, custom Trojan horse software, online banking information, eBay account usernames and passwords, PayPal accounts and others. The ShadowCrew apparently had 4,000 members working internationally [232]. It got hold of credit card details and other valuable information using different techniques such as sending millions of phishing emails, and hacking into databases. In 2004, just in one day and in one trade, one member of ShadowCrew sold 115,695 stolen credit card details [232]. In 2003, the USA Secret Service lunched Operational Firewall to catch the
suppliers of fake and stolen credit cards [232]. Because it was too big to hide, ShadowCrew attracted the Secret Service focus. After that, agents succeeded in snatching one of ShadowCrew members and convinced him to help them [232]. Later, that person helped the Secret Service set up a new electronic gateway to enter the ShadowCrew Website, then advise ShadowCrew members that the new gateway was more secure for entering their Website [232]. This step allowed the Secret Service to monitor all the ShadowCrew members’ communications which led to bringing down ShadowCrew in October 2004 [232].

**Holiday prize scam**

*Nicole* was surfing the Internet and a pop-up webpage appeared on her computer telling her that she had won a holiday prize to the Bahamas, and in order to retrieve her prize, she should call the number listed immediately [233]. *Nicole* called the listed number and a lady with an American accent answered the call and told her that she won a holiday prize and asked her if she accepted the holiday and she said yes. Then, the lady asked *Nicole* for her credit card details and after having taken *Nicole’s* credit card information the lady told *Nicole* that she is locked in to buying the holiday [233]. Then, *Nicole* realized that part of the prize cost had been charged to her credit card and asked to pull out, however, the lady refused. After that, Nicole talked with the manager who refused to let her withdraw from the holiday and told her that they will reduce the amount that they will take from US$680 to US$350 and *Nicole* can try to sell the holiday to another person [233]. Then, *Nicole* told the manager to wait for her husband to come back, but the manager told her if she hung up the phone, she would pay US$1,000 and she would be charged twice if she made a complaint [233]. *Nicole* contacted her bank to cancel her credit card and later on, the bank got her money back.

**Fraud and money laundering scheme**

During the period from 1999 to 2001, the Tri-West Investment Club attracted 15,000 investors and involved $60 million in investments [234]. The Tri-West solicited investments on the Internet using its Website ‘www.triwestinvest.com’. The investments were in a ‘Bank Debenture Trading Program’. The Tri-West Website offered investors a guaranteed high annual return of 120 percent without
any risk [234]. The Tri-West claimed it invested in buying ‘Promissory Bank Notes’ issued by key banks. The Tri-West Website notified the investors to invest by $1,000 increments. However, Tri-West was not a legitimate investment company and the ‘Bank Debenture Trading Program’ did not exist [234]. The Tri-West scheme used the recent investor funds to pay earlier investors as a return for their investments to give a fake impression of good investment income. The Tri-West staff gave false information for the investors. Later, the investigators found there was no investment as promised and the money had been used to purchase expensive properties and other items. Also, millions of the money was transferred to ‘shell’ corporations to conceal the illegal gains. In the end, the offenders were arrested for multiple charges and one of them pled guilty to mail fraud, wire fraud and conspiracy to commit money laundering [234].
Appendix B: CoE Convention on Cybercrime

Appendix B.1: Articles 2 to 11 of the CoE Convention on Cybercrime

Appendix B.1 states the Articles 2 to 11 of the CoE Convention on Cybercrime in detail.

Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
A Party may reserve the right to require that the conduct described in paragraph 1 results in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of Devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with the intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in
accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data,

b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.
Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system

b offering or making available child pornography through a computer system

c distributing or transmitting child pornography through a computer system

d procuring child pornography through a computer system for oneself or for another person

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term ‘child pornography’ shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conductrealistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term ‘minor’ shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.
Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party’s international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.
Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.
Appendix B.2: Detailed Analysis of the CoE Convention on Cybercrime

Appendix B.2 reviews and analyses Articles 2 to 11 of the CoE Convention on Cybercrime.

Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Illegal access to a computer and computer system is an essential element for committing further offences against the confidentiality, integrity and availability of computer data and systems. Examples of illegal access include hacking, cracking and computer trespass. The purpose of criminalising the illegal access is to provide additional protection for computer systems and data. The term ‘access’ covers the entering of the whole or part of computer systems, such as data, hardware, directories and traffic. The conduct of illegal access must be committed ‘intentionally’ and ‘without right’. There is no criminal intent when entering an open and free system that permits such access.

Article 3 – Illegal interception

Article 3 requires the member countries to implement legislation that protects the confidentiality of the computer data and systems. It intends to protect the right of the privacy of data communication. Article 3 makes illegal criminal interceptions without right, committed intentionally and using technical means and it applies to all forms of electronic data transfer including telephone, fax, e-mail and file-transfer. Also, technical means is a requirement to avoid ‘over-criminalization’ and includes technical devices to collect and record communications, software, passwords and codes. Article 3 provisions cover non-public transmissions of data which applies to the nature of the communication process and not the nature of the data, such as Pay TV and the communications of employees. Overall, this article imposes some challenges to be implemented and enforced by authorities in

---

22 See the CoE Explanatory Report to the Convention on Cybercrime no. 44.
23 See the CoE Explanatory Report to the Convention on Cybercrime no. 45.
24 See the CoE Explanatory Report to the Convention on Cybercrime no. 46.
25 See the CoE Explanatory Report to the Convention on Cybercrime no. 51.
26 See the CoE Explanatory Report to the Convention on Cybercrime no. 51.
27 See the CoE Explanatory Report to the Convention on Cybercrime no. 53.
28 See the CoE Explanatory Report to the Convention on Cybercrime no. 54.
order to avoid ‘over-criminalization’. It focuses only on the nature of the private communication process regardless of the nature of the data. For example, the emails between two company’s employees are protected under this article regardless of the purpose of these emails.

**Article 4 – Data interference**

Article 4 of the CoE Convention makes illegal data interference and requires the implementation of legislation that makes such interference an offence. It intends to protect the data integrity and to provide computer programs and data with protection\(^{29}\). The offence must be committed intentionally and without right. Article 4 provisions make illegal those acts of damaging, deletion, deterioration, alteration or suppression of computer data without right when committed intentionally. Malicious codes such as Viruses and Trojan horses are covered under this article for their harmful modification of computer data. Nevertheless, Article 4 also has some provisions on the authorized modification of data in the design of networks or other practices. The authorized modification for the testing or protection of the security purposes are not made illegal by Article 4\(^ {30}\). Additionally, Article 4 allows countries to include additional elements for the offence that includes requiring that the offence has resulted in serious harm\(^ {31}\). This part in particular could create some diversity in relation to the extent of the serious harm and how each country defines its criteria.

**Article 5 – System interference**

Article 5 makes illegal the system interference that is known as computer sabotage. It intends to protect the “legal interest of operators and users of computers or telecommunication systems being able to have them function properly”\(^ {32}\). Article 5 makes illegal the serious hindering of the functions of the computer systems including telecommunications facilities when it is committed intentionally and without right\(^ {33}\). Under Article 5, the term ‘hindering’ refers to “actions that interfere with the proper functioning of the computer system. Such

---

\(^{29}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 60.

\(^{30}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 62.

\(^{31}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 64.

\(^{32}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 65.

\(^{33}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 65.
hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data”\(^{34}\). Article 5 indicates that the hindering must be serious for it to be made illegal; however, it allows countries to determine what criteria considers hindering as serious. It can be observed that the reason behind this requirement is to avoid over-criminalization. For instance, sending a limited number of unsolicited emails could annoy the receivers but does not create any damage to their computer systems. Nevertheless, Article 5 intends to protect computer system from any harmful interference in order that the system functions properly. Some examples of system interference include Denial of Service (DoS) attacks\(^{35}\), malicious codes such as dissemination of viruses that prevent or slow the operations of the system and spam emails.

**Article 6 – Misuse of Devices**

Article 6 makes illegal the intentional commission of some unauthorized acts in relation to computer devices or access passwords, code or data that can be misused for committing any of the offences established in accordance with Articles 2-5\(^{36}\). The ultimate aim of this Article is to protect the confidentiality, integrity and availability of computer systems and data through reducing the availability of some ‘hacker tools’ or other tools\(^{37}\).

While some of the tools are dual-use devices that could be used for criminal or security-testing purposes, the second paragraph of Article 6 permits the use of such tools for the authorized testing or protection of a computer system. Article 6 requires the offence to be committed intentionally and without right to avoid ‘over-criminalization’\(^{38}\). In addition to the second paragraph of Article 6, the expression ‘without right’ covers the provisions for removing the criminal liability from using dual-use devices for the authorized testing of a computer system\(^{39}\). Additionally, the third paragraph of Article 6 allows countries the right not to apply the whole of the first paragraph except for the sale, distribution or otherwise...

---

\(^{34}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 67.

\(^{35}\) According to CERT, denial of service (DoS) attack is ‘characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service’.

\(^{36}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 71.

\(^{37}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 71.

\(^{38}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 76.

\(^{39}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 77.
making available of items mentioned in (1)(a)(ii)\textsuperscript{40}. It is submitted that this specific Article creates many legal issues in relation to making illegal the production and distribution of the dual-use tools, rather than the criminal conduct that results from using such tools. For instance, a person has some specific research related to identifying system and network vulnerabilities by using some dual-use devices, and they produce and make such devices available on their website. How can the authorities determine that this person only produces and makes such devices available for security purposes, and not for criminal purposes? Some researchers, such as Kierkegaard (2007) \textsuperscript{[315]}, believe that this Article could affect the development of new security tools. In conclusion, there is a concern for how countries would determine whether the dual-use devices are used or will be used for legal or criminal purposes. This article, in fact, should focus on such devices whenever there are some criminal acts resulting from such use, not just from distributing or using these devices. But, what we observed is that this article focuses on dual-use tools not on the criminal conduct. As a result, many civil organisations, such as the Global Internet Liberty Campaign, objected to this article which could result in a bias to “investigate individuals engaged in computer-related activity that is completely lawful” \textsuperscript{[316]}.

\textit{Computer-related offences}

\textbf{Article 7 – Computer-related forgery}

The intent of Article 7 is to provide a protection for the electronic documents similar to the protection provided for tangible documents\textsuperscript{41}. The provision of Article 7 covers the unauthorized manipulation, creation or alteration of data resulting in non-authentic data with the intent of it being used for legal transactions and documents\textsuperscript{42}. The intention of the provision is to protect the legal interests of the security and reliability of electronic data, whether it is public or private data\textsuperscript{43}. Article 7 covers a wide range of provisions; however, it does not require countries to implement some important elements attached to the offence

\textsuperscript{40} See the CoE Explanatory Report to the Convention on Cybercrime no. 78.
\textsuperscript{41} See the CoE Explanatory Report to the Convention on Cybercrime no. 81.
\textsuperscript{42} See the CoE Explanatory Report to the Convention on Cybercrime no. 84.
\textsuperscript{43} See the CoE Explanatory Report to the Convention on Cybercrime no. 83.
of forgery\textsuperscript{44}, including the ‘intent to defraud’ or ‘dishonest intent’. It does allow them to choose whether or not to implement such obligations. There are some problems with this article. For example, users are required to provide authentic data for legal purposes, but the case is different when subscribing or registering for a website such as a dating site or a free email such as hotmail. Also, how much trust should be put on these websites or emails in order to provide our authentic information. Nowadays, people hear how private data is misused or exposed from legitimate business websites, therefore, what is the case with a free subscription website or email. They usually survive on advertisements and selling subscribers’ private data. Kierkegaard [315] indicated that Article 7 could allow companies to force subscribers to provide their private details or risk being reported for fraud.

\textbf{Article 8 – Computer-related fraud}

The intention of this article is to make illegal any unnecessary handling of data without right with the intention to defraud, and an unlawful transfer of property. This article makes illegal the acts of committing economic crimes such as fraud, including credit card fraud\textsuperscript{45}. Although fraud is considered as a crime in terms of criminal legislation, computer-related fraud is likely to involve unauthorized access and/or modification of computer data or programs [317]. To cover all related manipulations, Article 8 makes illegal the acts of inputting, altering, deleting or suppressing of data or any interference with a computer system\textsuperscript{46} that resulted in a direct property or economic loss (for example, loss of money, tangible or intangible with an economic value)\textsuperscript{47}. The illegal act must be committed without right and the economic gain must be obtained without right. Moreover, the illegal act also must be committed intentionally and with specific fraudulent or dishonest intent to obtain an economic benefit\textsuperscript{48}. The purpose of the previous conditions is to extract any criminal liability from the commercial practices that

\textsuperscript{44} According to the CoE Explanatory Report to the Convention on Cybercrime no. 82, “national concepts of forgery vary greatly. One concept is based on the authenticity as to the author of the document, and others are based on the truthfulness of the statement contained in the document. However, it was agreed that the deception as to authenticity refers at a minimum to the issuer of the data, regardless of the correctness or veracity of the contents of the data”.

\textsuperscript{45} See the CoE Explanatory Report to the Convention on Cybercrime no. 86.

\textsuperscript{46} See the CoE Explanatory Report to the Convention on Cybercrime no. 87.

\textsuperscript{47} See the CoE Explanatory Report to the Convention on Cybercrime no. 88.

\textsuperscript{48} See the CoE Explanatory Report to the Convention on Cybercrime no. 90.
are not committed with fraudulent or dishonest intent. Such practices could result in an economic benefit for a person and a loss to another. In contrast to Article 7 concerning computer-related forgery, Article 8 requires the intent to defraud to establish any criminal liability in relation to computer-related fraud. This, in fact, protects the users especially when they subscribe to a website or a free email without giving their private data.

**Content-related offences**

**Article 9 – Offences related to child pornography**

This Article intends to protect children from abuse and to combat the sexual exploitation of children and child pornography. It makes illegal the acts of producing, offering, making available (for example, uploading and creating child pornography sites, creating hyperlinks to child pornography)\(^{49}\), distributing, transmitting (for instance, sending child pornography material)\(^{50}\), procuring (as in, downloading)\(^{51}\) and possessing child pornography through or in a computer system. Article 9 requires the offence to be committed intentionally and without right. The term ‘without right’ does not exclude legal defences and countries are allowed to take into account certain circumstances\(^{52}\). For example, a country may allow the use of pornographic material for medical purposes only.

In general, Article 9 covers the broad provisions in relation to child pornography and the sexual exploitation of children. Nevertheless, most countries, including Australia, the UAE, the UK and the USA have provisions for child pornography and the sexual exploitation of children. However, Article 9 contains some debatable provisions. First, the term ‘without right’ is not required in this sense, because child pornography is commonly a crime with some exceptional circumstances that will, or will not, relieve a person from criminal liability, and that depends on each jurisdiction. Second, paragraph 2 (b) refers to three types of offence under the term ‘child pornography’; one is “a person appearing to be a

---

\(^{49}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 95.

\(^{50}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 96.

\(^{51}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 97.

\(^{52}\) According to the CoE Explanatory Report to the Convention on Cybercrime no. 103, ‘the term ‘without right’ allows a Party to take into account fundamental rights, such as freedom of thought, expression and privacy. In addition, a Party may provide a defence in respect of conduct related to ‘pornographic material’ having an artistic, medical, scientific or similar merit’.
minor engaged in sexually-explicit conduct”. However, a person aged 18 years in one country could appear, in another culturally different country, older or younger than that age. In reality, there are other factors that could contribute to a false judgment in relation to the age of a person, such as the person’s colour. Therefore, this paragraph 2 (b) is wide in meaning, and which may result in varying implementations of the provision. Some jurisdictions may decide to not apply it at all. Third, paragraph 2 (c) also applies the term ‘child pornography’ to realistic images, even if they are generated by a computer. Once again, how would a jurisdiction determine the age of this ‘realistic image’ merely from its appearance? It does not make sense, unless the image clearly shows the age of the person. Fourth, another important factor is that the age of a minor may be different from country to country; Article 9 has contributed to this confusion by allowing countries to lower the age of minors to under 16. That would result in having different ranges of the age from under 18 to under 16. That, then would result in having an act described as a crime in one jurisdiction and being legally allowed in another. This, position is not uncommon when it comes to cybercrime though harmonisation would be preferable.

Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

Article 10 intends to make illegal offences related to the infringements of intellectual property right and related rights (for example, literary, musical, audio-video) when they are committed ‘willfully’, using a computer system and on a commercial scale\(^{53}\). This type of criminal activity is becoming a major issue globally because organised crime groups have exploited the ease of copying digitised of copyright material and thus have made substantial illegal commercial gains in this area. In contrast to all other provisions of the CoE Convention, Article 10 does not require that the offence must be committed intentionally; however, it does require the offence to be committed ‘wilfully’\(^{54}\). The provisions of committed

\(^{53}\) See the CoE Explanatory Report to the Convention on Cybercrime no. 108.

\(^{54}\) According to the CoE Explanatory Report to the Convention on Cybercrime no. 113, the term ‘wilfully’ is “used instead of ‘intentionally’... as this is the term employed in the [Trade-Related
wilfully are intended to criminalise infringements on a commercial scale. Additionally, each country is required to apply agreements that it is a party to, as the term “pursuant to the obligations it has undertaken”, has indicated. This means that Article 10 was introduced to set obligations on countries according to their commitments to international agreements, to make illegal offences related to infringements of copyright and related rights when they are committed using a computer system. Therefore, regardless of the number and types of legislation introduced, Australia, the UAE, the UK and the USA need to satisfy at least three conditions to be aligned with Article 10 of the CoE Convention. These conditions require countries to have criminal provisions for offences related to infringements of copyright and related rights when they are committed, (1) using a computer system, (2) wilfully and, (3) on a commercial scale. In April, 2010, a draft of Anti-Counterfeiting Trade Agreement (ACTA) has been released which aimed to provide further protection to intellectual property through “improving enforcement international cooperation; establishing enforcement best practice; and enhancing the enforcement legal framework”. The ACTA targets individuals who are involved in counterfeit and infringements of copyrights in commercial scale trade.

**Ancillary liability and sanctions**

**Article 11 – Attempt and aiding or abetting**

The intention of Article 11 is to establish additional offences in relation to aiding, abetting or attempting the commission of any of the cybercrime offences established under Articles 2 to 10. While countries are especially required to make illegal the aiding or abetting of the commission of cybercrime offences, they are not required to make illegal the attempt to commit any of the offences. Nevertheless, such aiding, abetting or attempting must be committed intentionally. It is important to remove any criminal liability from a party that does not have any knowledge or intention for a crime to be committed.
instance, the CoE Convention indicated that in cases when customers transmitted malicious codes or illegal contents through an Internet Service Provider's (ISP) services, the ISP cannot hold any criminal liability when it does not have criminal intent or knowledge\textsuperscript{58}. This is because there is no responsibility on the ISP to monitor content transferred through its servers. Therefore, countries may impose some obligations on the ISPs to monitor their customers or third party content which could result in monitoring of private communications [316]. Nevertheless, the ISPs do not want to monitor the contents transferred through their servers due to the administration costs involved not just for privacy issues.

\textsuperscript{58} See the CoE Explanatory Report to the Convention on Cybercrime no. 119.
Appendix B.3: Detailed Analysis of the Existence and Alignment of Computer Crime or Cybercrime Legislation Relating to the CoE Convention in Australia, the UAE, the UK and the USA

This appendix consists of a comparative review of the computer crime or cybercrime legislation used in Australia, the UAE, the UK and the USA that align with Articles 2 to 11 of the CoE Convention.

Article 2 – Illegal access

Australia

In Australia, Section 478.1 of the Criminal Code (Cth) makes illegal the unauthorized access to, or modification of, restricted data, when committed intentionally and with the knowledge that the access or modification is unauthorized. The illegal access offence is punishable under Section 478.1 with two years imprisonment. Additionally, Section 477.1 makes illegal the unauthorized access, modification or impairment with intent to commit a serious offence. Section 477.1 indicates other elements attached to the offence of illegal access, such as data modification.

UAE

Article 2 of the UAE Federal Law No (2) of 2006 makes illegal any intentional act of unauthorised access to a computer system or website without authorization or the breaking through of security measures. The penalty is a fine and/or imprisonment. If such act results in the deletion or alteration or other harmful intent or the data is personal, the penalty is a minimum of a one-year imprisonment and/or a fine.

UK

The Computer Misuse Act 1990 of the UK makes illegal the unauthorised access to computer material. Section 1 of the Act makes illegal the intent to commit unauthorized access to any computer program or data or to enable such access. The punishment imposed is for a term not exceeding two years imprisonment.

59 Under Div 478.1 (3), "restricted data means data: (a) held in a computer; and (b) to which access is restricted by an access control system associated with a function of the computer".
and/or a fine. Section 2 of the Act makes illegal the access with intent to commit or facilitate the commission for further offences.

**USA**

Section 1030 of Title 18 of the USA Code, also known as the ‘Computer Fraud and Abuse Act’, has a number of offence provisions that apply to illegal access and fraud in connection with computers. Sections 1030(a) (1) - (5) make illegal the act of intentionally accessing a protected computer without authorization or exceeding the authorization with the intent to commit other offences, such as defraud and obtaining data. The punishment is a fine and/or a maximum of ten years imprisonment. For instance, see *United States v. Phillips*, 2007 [319]. Phillips was a student at the University of Texas. He used his computer account to scan computer networks and steal data and passwords including credit card numbers and Social Security numbers. Phillips was found guilty and convicted of one count of unauthorised access to commit computer fraud under Section 1030(a)(5) and another “count of possession of an identification document containing stolen Social Security numbers” under Section 1028(a)(6).

**Summary**

The cybercrime legislation of Australia, the UAE, the UK and the USA does not demand the requirement of illegal access ‘in relation to a computer system that is connected to another computer system’. Also, the UK and the USA do not demand the requirement of ‘infringing security measures’. Moreover, Article 2 does not require countries to provide such requirements. It appears that Australia, the UAE, the UK and the USA are fully in alignment with the CoE Article 2 provisions on the criminal act of illegal access to computer systems. Table B1 illustrates this result.

---

60 Under the U.S. Code, Title 18, Section 1030 (e) 2, the term ‘protected computer’ means “a computer (a) exclusively for the use of a financial institution or the United States government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offence affects that use by or for the financial institution of the Government; or (b) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.”
Table B1 CoE provisions for illegal access and the related provisions and alignment from Australia, the UAE, the UK and the USA

<table>
<thead>
<tr>
<th>Conditions that must be satisfied to be in alignment</th>
<th>CoE – Article 2</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without right</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Committed intentionally</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Infringing security measures</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Intent to obtain computer data or other dishonest intent</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>In relation to a computer system that is connected to another computer system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Any or all of the additional elements of illegal access</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alignment with CoE Article 2</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Article 3 – Illegal interception**

**Australia**

The Telecommunications (Interception and Access) Act 1979 (Cth) criminalises illegal interception. Under Part 2-1 of the Telecommunications Act, subsection 7 (1) prohibits illegal interception of a telecommunications system. Subsection 105 (2) of the Telecommunications Act indicates that an offence against subsection 7 (1) is punishable by a maximum of two years imprisonment. However, there is no requirement that the offence is committed using any technical means, such as codes or passwords. Moreover, there is no requirement that the offence must be committed ‘with dishonest intent’ and ‘in relation to a computer system that is connected to another computer system’. The punishment for illegal interception is two years imprisonment. Also, Section 477.1 makes illegal the unauthorized access, modification or impairment with intent to commit a serious Commonwealth, State or Territory offence.

**UAE**

In the UAE, Article 8 of the Federal Law makes illegal the interception without authorization when it is committed intentionally. The Article states that the person is guilty of an offence if they eavesdrop, receive or intervene with information sent via the Internet or high-tech devices. The UAE does not impose some of the CoE requirements, such as that, the offence must be committed by ‘technical means’, it
applies to ‘non-public transmissions’, with ‘dishonest intent’ or ‘in relation to a computer system that is connected to another computer system’. The illegal interception is punished with a fine and/or imprisonment.

**UK**

Section 1 of the Computer Misuse Act of the UK makes illegal the unauthorized access to computer material (data or program) when it is committed intentionally and with knowledge. Additionally, Section 2 makes illegal the unauthorized access with intent to commit or facilitate the commission for further offences, such as illegal interception. The Regulation of Investigatory Powers Act 2000 (RIPA) of the UK [320] has a number of provisions for the illegal interception. The RIPA makes illegal interception without right when committed intentionally. The offence is punished with a fine and/or a maximum of two years imprisonment. In contrast to the conditions of Article 3 of the CoE Convention concerning the interception without warrant and using technical means, the Regulation of Investigatory Powers Act 2000 makes illegal generally any unlawful interception to a public postal service and the public communication system during its transmission. In fact, the UK legislation does not recognise some of the CoE requirements, such as the offence must be committed by ‘technical means’, with ‘dishonest intent’ or ‘in relation to a computer system that is connected to another computer system’.

**USA**

Sections 2510–2522 of Title 18 of the USA Code, also called ‘Wire and Electronic Communications Interception and Interception of Oral Communications’, have a number of offence provisions for the interception and disclosure of wire, oral or electronic communications including computers. Section 2510 defines the ‘electronic communications system’ as, ‘any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications’. Section 2511 makes illegal the unauthorised interception and disclosure of wire, oral or electronic communications when it is intentionally committed using any electronic, mechanical or other device to intercept any business or commercial establishment
communications. The USA refers to ‘non-public transmission’ as, “any wire, oral or electronic communication”. The punishment for the illegal interception is a fine and/or a maximum of five years imprisonment. Section 2512 makes illegal the acts of manufacture, distribution, possession and advertising of wire, oral or electronic communication interception devices unless they are used in the normal course of the business or activities of the USA, a State or a political subdivision. Sections 2510–2522 make the USA legislation consistent with Article 3.

**Summary**

Unlike the USA legislation, the cybercrime legislation of Australia, the UAE and the UK does not demand the requirement of the illegal interception to be committed using technical means. Additionally, all criminal provisions in the above countries do not require additional elements for the offence, such as the offence committed ‘with dishonest intent’ and ‘in relation to a computer system that is connected to another computer system’. It seems that apart from the USA — which is aligned — Australia, the UAE and the UK are partially in alignment with Article 3 of the Convention. Table B2 demonstrates these findings.

Table B2 CoE provisions on illegal interception and the related provisions and alignment from Australia, the UAE, the UK and the USA

<table>
<thead>
<tr>
<th>Conditions that must be satisfied to be in alignment</th>
<th>CoE – Article 3</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without right</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Committed intentionally</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Made by technical means</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Non-public transmissions of computer data to, from or within a computer system including electromagnetic emissions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additional elements of illegal interception</th>
<th>CoE – Article 3</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committed with dishonest intent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In relation to a computer system that is connected to another computer system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Alignment with CoE Article 3 | No | No | No | Yes |
Article 4 – Data interference

Australia

The Cybercrime Act 2001 of Australia, Divs 477 and 478 of the Criminal Code (Cth), cover all forms of data interference. Section 477.2 has provisions on the unauthorized modification of data to cause the impairment of accessing the data held in any computer or the reliability, security or operation of any such data. Section 477.2 does require the offence to be committed intentionally. The punishment is imprisonment for a maximum of ten years. Under Section 476.1 of the Criminal Code (Cth), the term ‘modification’ means, “(a) the alteration or removal of the data; or (b) an addition to the data”. While Australia does not use the same words of the Article 4 provision, it still covers the alteration, deletion or addition of computer data. The provision under the term ‘modification’ includes an addition to the data that could result in a negative alteration of the data, which is the same provision provided under the terms ‘damaging’ and ‘deterioration’. Additionally, Section 478.2 makes illegal the unauthorized impairment of data held on a computer disk or credit card or another device used to store data by electronic means. Section 478.2 establishes some requirements for the offence to be committed intentionally, without right and with knowledge. The illegal system interference under Section 478.2 is punishable with two years imprisonment.

UAE

With regard to the UAE legislation, Articles 2 and 6 of the Federal Law have provisions for illegal data interference. Article 2 makes illegal any intentional acts of unauthorized deletion, erasure, destruction, disclosure, damaging, alteration or republication of computer information or data. Article 6 not only has provision for data protection, but also exceeds that to cover the protection of computer information, data and programs from unauthorized disabling, disruption, destroying, deletion, damaging or modification. Article 2 and 6 make the UAE legislation consistent with Article 4 of the CoE Convention. The punishment for this offence is a fine and/or imprisonment.
UK

In the UK, the Computer Misuse Act 1990 and the Data Protection Act 1998 make illegal any unlawful data interference. Section 3 of the Computer Misuse Act has prohibited unauthorized acts with intent to impair with a computer. The mandatory intent is described below under Section 3(2) of the Act:

The person intends by doing the act – (a) to impair the operation of any computer; (b) to prevent or hinder access to any program or data held in any computer; or (c) to impair the operation of any such program or the reliability of any such data; or (d) to enable any of the things mentioned in paragraphs (a) and (c) above be done.

The above description covers the damaging (impairing) and suppression (preventing and hindering) access to any program and data held in a computer. These provisions are designed to cover DoS attacks. Additionally, the Act notes that the modification of the contents takes place if “(a) any program or data held in the computer concerned is altered or erased; or (b) any program or data is added to its contents”. The UK Computer Misuse Act covers the alteration, deletion and addition to computer data or program. Under the UK Computer Misuse Act, the data interference offence is punished with a fine and/or a maximum of ten years imprisonment.

USA

Section 1030 of Title 18 of the USA Code makes illegal the unlawful data interference. Section 1030 (a)(5) have provisions on data interference offences and it reads that whoever:

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss ... shall be punished.
Under Section 1030, the term ‘exceeds authorized access’ means “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter”, and the term ‘damage’ means “any impairment to the integrity or availability of data, a program, a system, or information”. The intent of Article 4 of the Convention is to protect the data integrity; therefore, the previous expressions under Section 1030 cover all the acts of damaging, deletion, deterioration, alteration or suppression of computer data without authorization. The punishment for the data interference offence is a fine and/or imprisonment.

**Summary**

It appears that Australia, the UAE, the UK and the USA are in alignment with the CoE Article 4 provisions for making criminal the act of illegal data interference. Table B3 illustrates this result.

Table B3 CoE provisions for data interference and the related provisions and alignment from Australia, the UAE, the UK and the USA

<table>
<thead>
<tr>
<th>Conditions that must be satisfied to be in alignment</th>
<th>CoE – Article 4</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without right</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Committed intentionally</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Damaging or deterioration of computer data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Deletion of computer data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Alteration of computer data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Suppression of computer data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Additional element of data interference</td>
<td>Resulted in serious harm</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alignment with CoE Article 4</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Article 5 – System interference**

**Australia**

In Australia, illegal system interference is made illegal under Sections 477.1, 477.3 and 474.14 of the Criminal Code (Cth). Section 477.1 makes illegal the acts of unauthorized access, modification or impairment with intent to commit a serious
offence. Section 477.3 makes illegal the unauthorized impairment of electronic communication to or from a computer when it is committed with knowledge. Section 477.3 makes illegal the creation of DoS attacks. Again, no intention is required under Section 477.3. The offence is punishable with imprisonment for ten years. Furthermore, DoS attacks and any suppression of computer data and programs are made illegal under Section 474.14. Section 474.14 covers the use of a telecommunications network with intention to commit a serious offence against a Law of the Commonwealth, a State or a Territory or a foreign law. The punishment for system interference under Section 474.14 is a penalty not exceeding the penalty applicable to the serious offence. In 2006, the Australian High Technology Crime Centre (AHTCC) reported that a man had been charged with ‘botnet’ and Distributed DoS attacks-related activities under Section 474.1. In conclusion, Sections 477.1, 477.3 and 474.14 cover all the acts of hindering without right the functioning of a computer system by inputting, damaging, deleting, deteriorating, altering or suppressing computer data.

**UAE**

Articles 5 and 6 of the UAE Federal Law have provisions for system interference. Article 5 makes illegal the acts of hindering or delaying access to a computer system, program, service or data. In contrast to Article 5 of the Convention, the UAE legislation does not demand some requirements, such as the crime must be committed intentionally, without right and resulted in serious hindering. Article 6 of the UAE Federal Law makes illegal the acts of insertion, modification, deletion and destroying of computer information, data or programs. These acts are punishable with a fine and/or imprisonment. While Article 6 also has some provisions for illegal system interference, it does not require the crime to be committed intentionally, without right and resulting in serious hindering. The punishment for illegal system interference is a fine and/or imprisonment.

---

61 Under Section 477.1 (9), serious offence means “an offence that is punishable by imprisonment for life or a period of 5 or more years”.

62 Under Section 473.2, serious offence against a foreign law means “an offence against a law of a foreign country constituted by conduct that, if it had occurred in Australia, would have constituted a serious offence against a law of the Commonwealth, a State or a Territory”.

63 See Section 474.14 (3).
**UK**

As indicated in the previous section, the UK legislation has provisions for the unauthorized modification of the contents of any computer when it is committed intentionally to impair the operation of any computer or to prevent or hinder access to any program or data. Section 3 of the Computer Misuse Act 1990 makes illegal the unauthorized acts with intent to impair, or with recklessness as to impairing, the operation of a computer. These provisions cover the damaging of computer operations and the suppression of access to any program and data held in a computer that would result in illegal system interference. The punishment for the system interference offence is a fine and/or imprisonment for up to ten years.

**USA**

In addition to having provisions for illegal data interference, Section 1030 (a)(5) of Title 18 makes illegal any illegal system interference. Section 1030 (a)(5) makes the USA legislation consistent with Article 5 of the Convention. The punishment for unlawful system interference is a fine and/or a maximum of two years imprisonment. For instance, Chapter 3 referred to Robert Morris who released a worm in 1988 to measure the size of the Internet. However, the spreading mechanism in the worm resulted in creating a denial of service (DoS) attack and caused a major disruption to numerous networks and computer systems [226]. Morris was convicted of intentionally gaining unauthorised access to a Federal interest computer through spreading a worm (computer program) and his offence was under Section 1030 (a)(5) [18].

**Summary**

It seems that Australia, the UK and the USA are in alignment with the CoE Article 5 provisions on the criminal act of illegal system interference. In contrast, the UAE is not aligned with the Article 5 requirements. Table B4 presents these findings.
Table B4 CoE provisions for system interference and the related provisions and alignment from Australia, the UAE, the UK and the USA

<table>
<thead>
<tr>
<th>Conditions that must be satisfied to be in alignment</th>
<th>CoE – Article 5</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serious hindering&lt;sup&gt;64&lt;/sup&gt;</td>
<td>Inputting computer data</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>Transmission computer data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Damaging or deterioration of computer data</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>Deletion of computer data</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>Alteration of computer data</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>Suppression of computer data</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>

Alignment with CoE Article 5

Yes  No  Yes  Yes

<sup>64</sup> It is up to each individual country to define the criteria on how to determine serious hindering; therefore, we believe that all of the above countries are alignment with Article 5 of the Convention in this perspective. See the CoE Explanatory Report to the Convention on Cybercrime no. 67.

<sup>65</sup> Under the Cybercrime Act 2001 (Section 476.1 of the Criminal Code Act 1995 (Cth)), the term ‘data’ includes “(a) information in any form; or (b) any program (or part of a program)”.

**Article 6 – Misuse of Devices**

**Australia**

In Australia, Sections 478.3 and 478.4 of the Criminal Code (Cth) cover the misuse of data (information in any form, program)<sup>65</sup> with intent to commit or facilitate the commission of a computer offence against Div 477. Section 478.3 makes illegal the possession or control of data with the intent to commit or facilitate the commission of a computer offence. The second paragraph of Section 478.3 makes it criminal liability even if committing an offence is impossible: “[a] person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible”. Section 478.4 makes illegal the acts of producing, supplying or obtaining data with intent to commit or facilitate the commission of a computer offence. The punishment for such an offence is three years imprisonment. While Australia has indicated that Sections 478.3 and 478.4 are intended to be consistent with the CoE Convention on Cybercrime requirements, it uses only some of the expressions in accordance with Article 6 of the Convention, such as possession, producing, supplying or obtaining data.
According to the third paragraph of Article 6, countries are required to at least make illegal the sale, distribution or making available of computer devices or access data. Sections 478.3 and 478.4 do not have provisions on the sale of dual-use computer devices; however, it could be argued that the term ‘supply’ covers the sale of such devices. Additionally, in contrast to Article 6, these two sections do not require the offence to be committed without right. Our findings suggest that Australia is not in alignment with Article 6 of the Convention.

**UAE**

The UAE Federal Law does not have a direct provision for the unlawful production, sale, procurement for use, import, distribution or otherwise making available of a computer and access device to be used in committing computer offences. However, Article 23 can cover such offences under the term ‘assisting’ others to commit an offence. Article 23 of the UAE Law reads: “[a] person who incites, aids, or conspires with another person to commit any of the offences described in this Law where the offence occurs as a result of such incitement, aid or conspiracy shall be liable to the same penalty”. Nevertheless, the UAE legislation fails to cover most requirements of Article 6 of the Convention.

**UK**

The Computer Misuse Act 1990 of the UK makes illegal the acts of making, supplying or obtaining articles (programs or data)\(^66\) intending to be used in committing or assisting in the commission of one of the offences provided by the Act. Section 3A of the Act requires that such a program and data are to be used for the criminal purpose of committing or assisting in the commission of a computer offence. In contrast to the requirements of Article 6 of the Convention, the Computer Misuse Act does not require the offence to be committed without right. While the Act also does not make illegal the sale of dual-use articles, it could be argued that the term ‘supplying’ covers the sale of such articles. The punishment for the misuse of devices is a fine and/or a maximum of two years imprisonment.

\(^{66}\) Under Section 3A of the Computer Misuse Act 1990, ‘article’ includes “any program or data held in electronic form”.
USA

In the USA, Section 1030 of Title 18 makes illegal the misuse of devices for committing some different offences. Section 1030 (a)(5)(A) places a criminal liability on any person who “knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer”. In addition to Section 1030, Section 1029 makes illegal misuse of access devices for defrauding and committing other offences. Section 1029 has provisions on the production, use, traffic, possession, control or custody, offering, selling of one or more unauthorized access devices, that intentionally and knowingly, will be used in the commission of an offence.

In 2006, the USA [321] declared that it “reserves the right not to apply paragraphs (1)(a)(i) and (1)(b) of Article 6 ('Misuse of devices') with respect to devices designed or adapted primarily for the purpose of committing the offences established in Article 4 ('Data interference') and Article 5 ('System interference')”67. However, according to paragraph (3) of Article 6 of the convention, countries are permitted to reserve the right not to apply the first paragraph except for part (1)(a)(ii). Therefore, Section 1029 makes the USA legislation consistent with the Article 6 requirements. The punishment for an offence under Section 1029 is a fine and/or a maximum of twenty years imprisonment. Additionally, Section 2512 of the USA Code makes illegal the manufacture, distribution, possession and advertising of wire, oral or electronic communication intercepting devices. The punishment is a fine and/or a maximum of five years imprisonment.

Summary

It appears that the USA is in alignment with the CoE Article 6 provisions on the making illegal the act of the misuse of devices. In contrast, Australia, the UAE and the UK are not aligned with the Article 6 requirements. Table B5 illustrates the results.

67 See the Council of Europe, List of the declarations made by: United States.
Table B5 CoE provisions for misuse of devices and the related provisions and alignment from Australia, the UAE, the UK and the USA

<table>
<thead>
<tr>
<th>Conditions that must be satisfied to be in alignment</th>
<th>CoE – Article 6</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without right</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Committed intentionally</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Sale, distribution or making available&lt;sup&gt;68&lt;/sup&gt;</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Computer password, access code or similar data</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
</tbody>
</table>

| Additional elements                               |                 |           |     |    |     |
| Production, procurement for use or import         |                 |           | √   | √  |     |
| Device including a computer program               |                 |           | √   | √  |     |
| Possession of an item mentioned above             |                 |           | √   | √  |     |

| Alignment with CoE Article 6                      | No              | No        | No  | Yes|

**Article 7 – Computer-related forgery**

**Australia**

Though Sections 477.2 and 478.2 of the Australian Criminal Code (Cth) have some provisions on unauthorized modifications and the impairments of data with intent to commit a computer offence, Div 144 and Div 145 makes illegal different acts in relation to forgery. Div 144 makes illegal the creation of false documents with the intention to be used as authentic documents to obtain gain<sup>69</sup>. Also, Div 145 makes illegal the following acts when they are committed intentionally and with knowledge, using a forged document, possession of a forged document, possession, making or adaptation of devices for making forgeries and falsification of documents. The punishment for such acts is 10 years imprisonment. While Div 144 and 145 require the offence to be committed intentionally, they do not require the offence to be committed without right. This is in contrast to the requirements of

---

<sup>68</sup> Third paragraph of Article 6 allows countries the right to not apply all the acts mentioned in the first paragraph, except the sale, distribution or making available of the items mentioned in (1)(a)(ii). See the CoE Explanatory Report to the Convention on Cybercrime no. 78.

<sup>69</sup> Part 3 of Section 144.1 reads: “A person is guilty of an offence if: (a) the person makes a false document with the intention that the person or another will use it: (i) to dishonestly cause a computer, a machine or an electronic device to respond to the document as if the document were genuine; and (ii) if it is so responded to, to dishonestly obtain a gain, dishonestly cause a loss, or dishonestly influence the exercise of a public duty or function; and (b) the response is in connection with the operations of a Commonwealth entity”. 
Article 7 of the Convention. However, that could be solved through Section 477.1 that makes illegal the unauthorized access, modification or impairment with intent to commit a serious Commonwealth, State or Territory offence such as forgery. Therefore, Australia is in alignment with Article 7 requirements.

**UAE**

With regard to the UAE legislation, Article 4 makes illegal the forging of any federal or local government documents of any federal or local institutions. The punishment is a fine and/or imprisonment. Additionally, Article 6 makes illegal the insertion of whatever can cause the modification, deletion, destruction of computer information, data or programs. The punishment for such an offence is a fine and/or imprisonment. Article 7 makes illegal the use of an electronic device for changing or destroying medical tests or facilitating others to do so. These acts are punishable with a fine or imprisonment. The previous Articles do not cover two important elements that must be attached to the offence, committed intentionally and without right. Article 10 makes illegal the use of a false name or impersonation with intent to defraud. The punishment is a fine and/or imprisonment for at least one year. The UAE legislation is not in alignment with Article 7 of the Convention.

**UK**

In the UK, the Computer Misuse Act 1990 makes illegal the unauthorized modification of the computer data and programs. Section 2 of the Act makes illegal the acts of unauthorized access with intent to commit or facilitate the commission of further offences. Additionally, the Forgery and Counterfeiting Act 1981 has strong penalties for forgery and related offences. The punishment is imprisonment for up to five years.

**USA**

Sections 1029 and 1030 of Title 18 of the USA Code have provisions on fraud and related activity in connection with computers and access devices. Section 1030

---

70 Under Section 3 of the Computer Misuse Act 1990, "[t]his section applies to offences – (a) for which the sentence is fixed by law; or (b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years".
covers all the acts of damaging, deletion, deterioration, alteration or suppression of computer data without right when they are committed intentionally and with knowledge. The punishment is a fine and/or imprisonment. Also, Section 1029 makes illegal the abuse of access devices for defrauding and committing other offences. Moreover, Section 1028 has provisions on fraud and related activity in connection with identification documents, authentication features and information. It creates criminal liability for any person who knowingly and without right produces, transfers, possesses, uses or traffics in false identification. Section 1037 covers provisions for fraud and related activity in connection with electronic email including forgery. Additionally, Chapter 25 of Title 18 of the USA Code covers a wide range of provisions concerning counterfeiting and forgery. Regarding the additional elements, the USA declared that it had attached the requirement of intent to defraud to the computer-related forgery. The USA legislation is aligned with all the requirements of Article 7 of the convention.

**Summary**

It seems that Australia, the UK and the USA are aligned with the CoE Article 7 provisions on the criminal act of illegal data interference. However, the UAE is not in alignment with the requirements of Article 7. Table B6 shows these findings.

Table B6 CoE provisions for computer-related forgery and the related provisions and alignment from Australia, the UAE, the UK and the USA

<table>
<thead>
<tr>
<th>Conditions that must be satisfied to be in alignment</th>
<th>CoE – Article 7</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without right</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Committed intentionally</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Input, alteration, deletion, or suppression of computer data resulting in inauthentic data</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Additional element Intent to defraud or dishonest intent</td>
<td>√</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Alignment with CoE Article 7</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

---

71 See Section 1037 (a)(5).
72 See the Council of Europe, List of the declarations made by: United States.
Article 8 – Computer-related fraud

Australia

The Australian Criminal Code (Cth) has provisions for computer-related fraud. Section 477.1 of the Criminal Code makes illegal the acts of unauthorized access, modification or impairment with intent to commit a serious offence against a law of the Commonwealth, a State or a Territory. In fact, Section 477.1 is designed to cover the illegal use of a computer system to commit serious crimes such as fraud. The computer-related fraud is punishable by a penalty not exceeding the penalty applicable to fraud under Div 134 and Div 135. Div 134 and Div 135 of the Criminal Code (Cth) make illegal the acts of obtaining property or a financial advantage and other offences involving fraudulent conduct. This offence is punished with imprisonment from twelve months up to ten years. While Section 477.1 covers most of the Article 8 requirements, it does not require the offence to be committed and the economic benefit must be obtained to convict. This, in fact, is in contrast to one of the main requirements of Article 8 of the Convention. Therefore, we find that Australia is not aligned with all of the Article 8 requirements.

UAE

Articles 10 and 11 of the UAE Federal Law have provisions for computer-related fraud. Article 10 makes illegal the use of the Internet or any high-tech devices for defrauding and obtaining funds or documents using deception or false identifications with intent to defraud. Article 11 also makes illegal the intentional use of the Internet or any high-tech devices to the unauthorized access of data or credit cards or any form of electronic cards for the purpose of defrauding and the unlawful obtaining of funds or other services attached to the card. In contrast to Article 8 of the Convention, Articles 10 and 11 of the UAE law cover the broad use of the Internet and any high-tech devices and do not specify some acts that are related to data manipulation and interference. Additionally, and likewise Australia, the UAE creates criminal liability even if the perpetrator does not obtain any financial gain. However, if the financial gain was obtained, then the punishment

---

would be tougher. This offence is punished by a fine and/or a minimum of a one-year imprisonment. The UAE legislation is not aligned with Article 8 of the Convention.

**UK**

In the U.K., Section 2 of the Computer Misuse Act 1990 makes illegal the unauthorized access with intent to commit or facilitate the commission of further offences such as fraud. While Section 2 requires the offence to be committed intentionally and without right, it does not require the offence to be committed. Section 2(4) reads, “[a] person may be guilty of an offence under this section even though the facts are such that the commission of the further offences is impossible”. This is in contrast to the Article 8 requirements. Nevertheless, Section 2 does not cover any illegal acts of data interference or modification; it covers only the unauthorized access offence. The offence is punishable with a fine and/or imprisonment for up to five years. Additionally, the Fraud Act 2006 of the UK [322] covers most different types of fraud, such as fraud by false representation, fraud by failing to disclose information and fraud by abuse of position. Sections 6 and 7 of the Fraud Act make illegal the acts of possession, making or supplying articles (program or data held in electronic form) for use in frauds74. The offence is punishable with a fine and/or imprisonment for up to ten years.

**USA**

The USA legislation is fully consistent with Article 8 of the Convention. Sections 1029 and 1030 of Title 18 of the USA Code have provisions on fraud and related activity in relation to computers. As indicated previously, Section 1030 makes illegal the acts of unauthorized access and unauthorized modification of computer data, when these acts are committed intentionally and without right. It makes illegal the unauthorized access or exceeding the authorization to a protected computer with intent to defraud and obtain anything of value. Section 1030 (a)(4) reads, whoever “knowingly and with intent to defraud, accesses a protected

---

74 According to the Fraud Act, the term 'Article' means “[f]or the purposes of - (a) sections 6 and 7, and (b) the provisions listed in subsection (2), so far as they relate to articles for use in the course of or in connection with fraud, 'article' includes any program or data held in electronic form”.
computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value”. The punishment for the computer-related fraud is a fine and/or up to five years imprisonment. Section 1029 also makes illegal the misuse of access devices with the intent to defraud and committing other offences. The offence is punishable with a fine and/or up to ten years imprisonment. Additionally, Section 1343 has a provision for using wire, radio and television to defraud or for obtaining money or property and the punishment for such an offence is a fine and/or up to twenty years imprisonment.

**Summary**

It appears that apart from the USA, which is in alignment with CoE Article 8 requirements, Australia, the UAE and the UK are not aligned with these requirements. Table B7 illustrates this result.

Table B7 CoE provisions for computer-related fraud and the related provisions and alignment from Australia, the UAE, the UK and the USA

<table>
<thead>
<tr>
<th>Conditions that must be satisfied to be in alignment</th>
<th>CoE – Article 8</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without right</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Committed intentionally</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Input, alteration, deletion, or suppression of computer data resulting in inauthentic data</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Fraudulent or dishonest intent</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Economic benefit must be obtained</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Alignment with CoE Article 8**

<table>
<thead>
<tr>
<th>Conditions that must be satisfied to be in alignment</th>
<th>CoE – Article 8</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without right</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Committed intentionally</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Input, alteration, deletion, or suppression of computer data resulting in inauthentic data</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Fraudulent or dishonest intent</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Economic benefit must be obtained</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Article 9 – Offences related to child pornography**

**Australia**

In Australia, the Criminal Code (Cth) covers offences relating to child abuse and pornography. Section 473.1 defines the term ‘child’ as a “person, who is, or appears to be, under 18 years of age”. Section 474.19 makes illegal the intentional use of a carriage service to access, transmit, make, publish or distribute child pornography material. The punishment is imprisonment for ten years. Additionally, Section 474.20 makes illegal the intentionally-committed acts of
possessing, controlling, producing, supplying or obtaining child pornography material for use via a carriage service. The offence is punishable with a ten-years imprisonment. Furthermore, Section 233BAB of the Customs Act 1901 (Cth) [323] has provisions for importing child pornography material into Australia. In conclusion, Sections 474.19 and 474.20 are consistent with Article 9 of the Convention.

**UAE**

Articles 12 and 13 of the UAE Federal Law have provisions for the exploitation of minors and child pornography. The UAE Civil Code defines a minor as a person under the age of 16. Article 12 makes illegal the sexual exploitation of minors. Article 13 also makes illegal the use of the Internet or any high-tech device for producing, preparing, sending or storing with the intent of exploiting, distributing or showing others sexual material and encouraging the sexual exploitation of minors. The punishment is a fine and six-month imprisonment. Article 13 also makes illegal the use of the Internet or high-tech devices for encouraging, assisting or deceiving of a minor to commit adultery or prostitution acts. The punishment for such offence is a fine and imprisonment for not less than five years.

**UK**

With regard to the UK legislation, the Protection of Children Act 1978 [324] and Sexual Offences Act 2003 [325] make illegal the acts of abusing minors and child pornography. The Protection of Children Act 1978 makes illegal the taking, making, distributing and possession of sexually-explicit images involving children. The punishment is a fine and/or up to ten years imprisonment. Section 45 of the Sexual Offences Act amends the meaning of ‘child’ from “persons under 16” to “persons under 18”. The provision makes illegal a wide range of offences relating to children. Sexual activity with a child is punishable with an imprisonment of up to fourteen years. Additionally, Sections 160 and 161 of the Criminal Justice Act 1988 makes illegal the act of possession of indecent photographs of children.

**USA**

The USA legislation is consistent with Article 9 of the Convention regarding the protection of minors from exploitation. Section 2256 defines the term ‘minor’ as
“any person under the age of eighteen years”. Sections 2251, 2252 and 2252A of Title 18 of the USA Code have provisions on offences related to child pornography committed with intent and knowledge. Section 2251 makes illegal the acts of employing, using, persuading, inducing, enticing and coercing of any minor to engage in any sexually explicit conduct. The offence is punished with a fine and imprisonment for fifteen to thirty years. Section 2252 makes illegal transporting, receiving, distributing, producing, supplying, and possessing child pornography through any means including by computer. The punishment for such an offence is a fine and imprisonment for five to twenty years. Section 2252A makes illegal the receiving, distributing, advertising, promoting, presenting, selling, possessing, accessing child pornography or any material that contains child pornography. The punishment ranges from five to twenty years imprisonment and/or a fine. For instance, see United States vs. Kuchinski, who had a count of receipt of child pornography in violation of Section 2252A (a)(2) and another count of possession of child pornography under Section 2252A (a)(5)(B), and a third count under Section 2253 for forfeiture of his computer [319].

**Summary**

It seems that Australia, the UAE, the UK and the USA are aligned with Article 9 provisions on the offences related to child pornography as shown in Table B8.

**Article 10 – Offences related to infringements of copyright and related rights**

**Australia**

In Australia, the Copyright Act 1968 (Cth) [326] deals with the infringement of copyright and related rights. The Act under very specific circumstances makes it a criminal offence to infringe copyright. Generally, the infringement even if deliberate will only amount to a civil matter and not a criminal matter. It is clearly understood that for an infringement to give rise to criminal sanctions the activity has to be a flagrant disregard to the copyright holders rights. It usually involves some deliberate commercial copying of material whether video material or software material. The offence if proved is punishable with a fine and/or imprisonment. With regard to committing infringements of copyright by means of
a computer system, the Criminal Code (Cth) has provisions for offences against copyrights and related rights. In fact, Section 477.1 of the Criminal Code makes illegal the acts of unauthorized access and modification with intent to commit a serious offence against a law of the Commonwealth, a State or a Territory. Therefore, Australia is in alignment with Article 10 requirements.

Table B8 CoE provisions for offences related to child pornography and the related provisions and alignment from Australia, the UAE, the UK and the USA

<table>
<thead>
<tr>
<th>CoE – Article 9</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committed intentionally</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Producing child pornography for distribution</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Offering or making available child pornography</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Distributing or transmitting child pornography</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The term 'child pornography' includes a minor engaged in sexually explicit conduct</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The term 'minor' includes all persons under 18 years of age. It is allowed to countries to have a lower age-limit but not less than 16 years</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Procuring child pornography</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Possessing child pornography</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The term 'child pornography' includes a person appearing to be a minor in sexually explicit conduct</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The term 'child pornography' includes realistic images representing a minor engaged in sexually explicit conduct</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Alignment with CoE Article 9</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**UAE**

The UAE Federal Law No 7 of 2002 regarding Copyright and Related Rights [327] covers all the offences of infringements of copyright and related rights. The punishment for copyright offences is a fine and/or imprisonment.
UK

In the UK, the Copyright, Designs and Patents Act 1998 [328] makes illegal the infringements of copyright and related rights and the reproduction, distribution, importation, selling or hiring of such protected rights. The offence is punishable with a fine and/or imprisonment for up to ten years. Moreover, Section 2 of the Computer Misuse Act 1990 makes illegal the unauthorized access with intent to commit or facilitate commission for further offences such as fraud and copyrights infringement.

USA

The USA legislation is consistent with Article 10 of the Convention regarding the protection of copyrights and related rights. Sections 1029 and 1030 of Title 18 have provisions for fraud and related activity in connection with computers and access devices. However, specific criminal provisions about the infringement of copyright and related rights are provided in Sections 506 and 2319 of the USA Code. Section 506 of Title 17 has provisions on criminal infringement of copyright and Section 2319 of Title 18 covers offences related to infringement of a copyright. The offence of infringement of copyright is punishable with a fine and/or imprisonment for up to ten years.

Summary

It appears that Australia, the UAE, the UK and the USA are in alignment with the CoE Article 10 provisions on the criminalization of offences related to infringements of copyright and related rights. Table B9 illustrate the findings.

Table B9 CoE provisions for computer-related forgery and the related provisions and alignment from Australia, the UAE, the UK and the USA

<table>
<thead>
<tr>
<th>Conditions that must be satisfied to be in alignment</th>
<th>CoE – Article 10</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisions on offences related to infringements of copyright and related rights committed by means of a computer system</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Committed wilfully</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Committed on a commercial scale</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Alignment with CoE Article 10</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Article 11 – Attempt and aiding or abetting

Australia

In Australia, the term ‘facilitate’ is being used to make illegal the intentional acts of ‘aiding’ or ‘abetting’ the commission of an offence\(^{75}\). Additionally, Div 477 and Div 478 of the Criminal Code (Cth) state that there is no offence in attempting to commit any of the offences established.

UAE

The UAE Federal Law covers the act of facilitating, aiding or enabling the commission of any of the offences listed under the law. In particular, Article 23 of the UAE Federal Law makes it an offence to incite, aid or conspire with another person for the commission of any of the cybercrime offences. However, and in contrast to Article 11 of the Convention, Article 23 of the UAE Law does not require the acts of inciting, aiding or conspiring to be committed intentionally.

UK

The UK legislation is consistent with the Article 11 requirements. Section 2 of the Computer Misuse Act 1990 makes illegal the acts of unauthorized access with intent to commit or facilitate the commission of further offences. Additionally, some sections of the Act such as 6, 9, 12 and 15 cover the general provisions concerning the attempt to commit one of the offences listed under Sections 1–3.

USA

In the USA, Section 2 of Title 18 has provisions for aiding or abetting the commission of an offence. Additionally, the attempt to commit an offence is covered by the USA legislation. Section 1030 (b) states that “[w]hoever conspires to commit or attempts to commit an offence under subsection (a) of this section shall be punished”. The USA legislation is in alignment with the requirements of Article 11 of the Convention.

\(^{75}\) For example, see the Cybercrime Act 2001, Div 477 and 478 of the Criminal Code (Cth).
**Summary**

It seems that Australia, the UK and the USA are in alignment with the CoE Article 11 provisions. In contrast, the UAE is not aligned with the requirements of Article 11. Table B10 shows these findings.

Table B10 CoE provisions for aiding, abetting or attempting the commission of any of the offences established under Articles 2–10 and the related provisions and alignment from Australia, the UAE, the UK and the USA

<table>
<thead>
<tr>
<th>Conditions that must be satisfied to be in alignment</th>
<th>CoE – Article 11</th>
<th>Australia</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committed intentionally</td>
<td></td>
<td>![ ](</td>
<td>)</td>
<td>![ ](</td>
<td>)</td>
</tr>
<tr>
<td>Aiding or abetting the commission of any of the offences established under articles 2–10</td>
<td>![ ](</td>
<td>)</td>
<td>![ ](</td>
<td>)</td>
<td>![ ](</td>
</tr>
<tr>
<td>Additional element</td>
<td></td>
<td>![ ](</td>
<td>)</td>
<td>![ ](</td>
<td>)</td>
</tr>
<tr>
<td>Attempting the commission of any of the offences established under articles 3, 4, 5, 7, 8, 9(1)(a) and 9(1)(c)</td>
<td>![ ](</td>
<td>)</td>
<td>![ ](</td>
<td>)</td>
<td>![ ](</td>
</tr>
</tbody>
</table>

Alignment with CoE Article 11 | Yes | No | Yes | Yes
Appendix C: Questionnaires and Interview Questions – Phase I

Appendix C.1: Questionnaires Questions – QPS and ADP

Note: the below form is intended for both QPS and ADP participants, except that for ADP participants we refer in the questions to ADP instead of QPS.

The Questionnaire Questions
Please answer as many questions as you can, and insert ‘not known’ or similar if you don’t know the answer to a question.

Please provide a response in the space allocated in the box under each question, or provide a reference to an available document which provides the response.

Introductory Questions

<table>
<thead>
<tr>
<th>Personal Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Interviewee contact details</td>
</tr>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Phone:</td>
</tr>
<tr>
<td>E-mail:</td>
</tr>
<tr>
<td>2 Organization details</td>
</tr>
<tr>
<td>Organization:</td>
</tr>
<tr>
<td>Position:</td>
</tr>
<tr>
<td>Job title:</td>
</tr>
<tr>
<td>Years in the police service:</td>
</tr>
<tr>
<td>Years in this position:</td>
</tr>
<tr>
<td>3 Questionnaire date and location of completion</td>
</tr>
<tr>
<td>Location:</td>
</tr>
<tr>
<td>Date of completion: / /2007</td>
</tr>
</tbody>
</table>
### Common Questions

The word ‘section’ in this part means the section where the interviewee actually operates.

<table>
<thead>
<tr>
<th>Common Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Considering the list of computer crimes listed below, what are the types of CC your section investigates? Please tick all that are applicable.</td>
</tr>
<tr>
<td>□ Unauthorized access (hacking; cracking)</td>
</tr>
<tr>
<td>□ Malicious code</td>
</tr>
<tr>
<td>□ Theft of service</td>
</tr>
<tr>
<td>□ Denial of Service (DoS) attacks</td>
</tr>
<tr>
<td>□ Credit card fraud</td>
</tr>
<tr>
<td>□ Online auction fraud</td>
</tr>
<tr>
<td>□ Online banking fraud</td>
</tr>
<tr>
<td>□ Child pornography</td>
</tr>
<tr>
<td>□ Online gambling</td>
</tr>
<tr>
<td>□ Spamming</td>
</tr>
<tr>
<td>□ Scams</td>
</tr>
<tr>
<td>□ Cyber stalking</td>
</tr>
<tr>
<td>□ Intellectual property</td>
</tr>
<tr>
<td>□ Copyrights crimes</td>
</tr>
<tr>
<td>□ Harassment</td>
</tr>
<tr>
<td>□ Social engineering fraud</td>
</tr>
<tr>
<td>□ Online identity theft</td>
</tr>
<tr>
<td>□ Online money laundering</td>
</tr>
<tr>
<td>□ Phishing</td>
</tr>
<tr>
<td>□ Electronic manipulation of sharemarkets</td>
</tr>
<tr>
<td>□ Forgery</td>
</tr>
<tr>
<td>□ Others:</td>
</tr>
</tbody>
</table>

2. Please identify the sections of relevant legislation under which investigation proceeds:

   (a) State legislation

   (b) Federal legislation

3. Is there a policy document which identifies the nature and role of the section? If so, please identify that document.

4. Does this section have specific procedures to investigate computer crimes? If
yes, please specify a summary of these procedures with reference to each of the crimes ticked in question one above, or provide a reference to the document(s) that specifies the procedures.

<table>
<thead>
<tr>
<th>5</th>
<th>From where does this section receive the computer incident complaint or request for investigation?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>e.g., from another section of the QPS, from another police service, from the public.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6</th>
<th>To whom does this section report the outcome of the investigation?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>e.g., to another section of the QPS, to another police service, to the public, to court.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7</th>
<th>How does the section report the outcome?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>e.g., specific forms used, written report, verbal report.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8</th>
<th>(a) Which of the crimes ticked in Q1 are investigated with or redirected to other sections? Which sections?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>e.g., online money laundering investigated by both Computer Crime Section and Proceeds of Crime Section, N/A.</td>
</tr>
</tbody>
</table>

|   | (b) How do the two or more sections manage or partition the investigation of the same crime? |

| 9 | (a) How long does this section on average take to start investigation after receiving the complaint? |

<p>|   | (b) How long on average after the investigation starts does the investigation take to conclude and report on investigation outcomes? |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Do any of the following challenges pose a potential problem for the section (tick all those that do):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>☐ Sufficient expertise to investigate diverse forms of CC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>☐ Sufficient staffing level</td>
<td></td>
</tr>
<tr>
<td></td>
<td>☐ Sufficient resources (e.g. equipments, budget, tools)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>☐ Sufficient training</td>
<td></td>
</tr>
<tr>
<td></td>
<td>☐ Cooperation with others law enforcement (e.g. national, international)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>☐ Cooperation with other organizations (e.g. private and public organizations)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>☐ Turnover of staff</td>
<td></td>
</tr>
<tr>
<td></td>
<td>☐ Jurisdictional problems with CC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>☐ Problems with the legislation relating to CC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>☐ Others:</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>For the section, what are the main issues that need to be addressed to improve the practice of combating CC?</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>How does the section upgrade and improve the skills of the personnel?</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Does this section require specific educational level to employ its personnel? If yes, please explain.</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Does the section have a comprehensive database for computer crime in QLD? If yes, please explain.</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>(a) Does this section educate the public about CC?</td>
<td></td>
</tr>
</tbody>
</table>
5. e.g., broadcasting TV advertisements, conducting seminars.

(b) If so, how.

Questions Related to each of the Four Sections

<table>
<thead>
<tr>
<th>The interviewee section</th>
</tr>
</thead>
<tbody>
<tr>
<td>In which section the interviewee operates:</td>
</tr>
<tr>
<td>☐ Computer Crime</td>
</tr>
<tr>
<td>☐ Identity Crime</td>
</tr>
<tr>
<td>☐ Proceeds of Crime</td>
</tr>
<tr>
<td>☐ Computer Forensics</td>
</tr>
</tbody>
</table>

Note: if the interviewee operates in more than one section, he/she should answer the related questions for all the ticked sections.
### 3.1 - Computer Crime

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>This question is about how the section deals with cases of “interstate” crimes. e.g., the offender, and the offence, and the complainant do not all reside in Queensland.</td>
</tr>
<tr>
<td>(a)</td>
<td>How are such crimes or complaints lodged with the section?</td>
</tr>
<tr>
<td>(b)</td>
<td>In which cases does QPS have jurisdiction?</td>
</tr>
<tr>
<td>(c)</td>
<td>In which cases does QPS not have jurisdiction?</td>
</tr>
<tr>
<td>(d)</td>
<td>In cases where QPS does not have jurisdiction, who does QPS refer the complaint to or deal with?</td>
</tr>
<tr>
<td>(e)</td>
<td>Are there jurisdictional problems resulting from different state’s legislation? If yes, please explain.</td>
</tr>
<tr>
<td>(f)</td>
<td>Please identify the relevant legislation:</td>
</tr>
<tr>
<td></td>
<td>a. State legislation</td>
</tr>
<tr>
<td></td>
<td>b. National legislation</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2</strong></td>
<td>This question is about how the section deals with cases of international crimes. e.g., the offender or the complainant resides overseas or the offence took place overseas.</td>
</tr>
<tr>
<td>(a)</td>
<td>How are such crimes or complaints lodged with the section?</td>
</tr>
</tbody>
</table>
(b) In which cases does QPS have jurisdiction?

(c) In which cases does QPS not have jurisdiction?

(d) In cases where QPS does not have jurisdiction, who does QPS refer the complaint to or deal with?

(e) Are there jurisdictional problems resulting from different international legislation? If yes, please explain.

(f) Please identify the relevant legislation:
   a. State legislation
   b. National legislation
   c. International legislation

3 Does the section prioritize by categories of crime? If yes, please explain. e.g., attacks on state information systems have a higher priority for crime investigation than if an individual’s system is attacked, the level of financial loss may affect prioritizing.

4 Amongst the cases you have dealt with, have there been cases where changes in legislation could have helped bring criminals to justice? If yes, please explain with a description of the problem and possible solution.
### 3.2 – Identity Crime

1. Please describe briefly the type of cases referred to the section.

2. This question is about how the section deals with cases of “interstate” crimes. e.g., the offender, and the offence, and the complainant do not all reside in Queensland.

   (a) How are such crimes or complaints lodged with the section?

   (b) In which cases does QPS have jurisdiction?

   (c) In which cases does QPS not have jurisdiction?

   (d) In cases where QPS does not have jurisdiction, who does QPS refer the complaint to or deal with?

   (e) Are there jurisdictional problems resulting from different state’s legislation? If yes, please explain.

   (f) Please identify the relevant legislation:

      a. State legislation

      b. National legislation

3. This question is about how the section deals with cases of international crimes. e.g., the offender or the complainant resides overseas or the offence took place
(a) How are such crimes or complaints lodged with the section?

(b) In which cases does QPS have jurisdiction?

(c) In which cases does QPS not have jurisdiction?

(d) In cases where QPS does not have jurisdiction, who does QPS refer the complaint to or deal with?

(e) Are there jurisdictional problems resulting from different international legislation? If yes, please explain.

(f) Please identify the relevant legislation:
   a. State legislation
   b. National legislation
   c. International legislation

Amongst the cases you have dealt with, have there been cases where changes in legislation could have helped bring criminals to justice? If yes, please explain with a description of the problem and possible solution.
### 3.3 – Proceeds of Crime

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Please describe briefly the type of cases referred to the section.</td>
</tr>
<tr>
<td>2</td>
<td>(a) How generally is “dirty money” identified? Please give a few examples.</td>
</tr>
<tr>
<td></td>
<td>(b) What specific techniques or mechanisms are used to trace back the dirty money to its origin?</td>
</tr>
<tr>
<td></td>
<td>(c) What difficulties are there to trace back the dirty money to its origin?</td>
</tr>
<tr>
<td>3</td>
<td>This question is about how the section deals with cases of “interstate” crimes. e.g., the offender, and the offence, and the complainant do not all reside in Queensland.</td>
</tr>
<tr>
<td></td>
<td>(a) How are such crimes or complaints lodged with the section?</td>
</tr>
<tr>
<td></td>
<td>(b) In which cases does QPS have jurisdiction?</td>
</tr>
<tr>
<td></td>
<td>(c) In which cases does QPS not have jurisdiction?</td>
</tr>
<tr>
<td></td>
<td>(d) In cases where QPS does not have jurisdiction, who does QPS refer the complaint to or deal with?</td>
</tr>
<tr>
<td></td>
<td>(e) Are there jurisdictional problems resulting from different state’s legislation? If yes, please explain.</td>
</tr>
<tr>
<td></td>
<td>(f) Please identify the relevant legislation:</td>
</tr>
<tr>
<td></td>
<td>a. State legislation</td>
</tr>
</tbody>
</table>
Appendix C: Questionnaires and Interview Questions – Phase I

4. This question is about how the section deals with cases of international crimes.
e.g., the offender or the complainant resides overseas or the offence took place overseas.

(a) How are such crimes or complaints lodged with the section?

(b) In which cases does QPS have jurisdiction?

(c) In which cases does QPS not have jurisdiction?

(d) In cases where QPS does not have jurisdiction, who does QPS refer the complaint to or deal with?

(e) Are there jurisdictional problems resulting from different international legislation? If yes, please explain.

(f) Please identify the relevant legislation:

   a. State legislation

   b. National legislation

   c. International legislation

5. Amongst the cases you have dealt with, have there been cases where changes in legislation could have helped bring criminals to justice? If yes, please explain with a description of the problem and possible solution.
### 3.4 - Computer Forensics

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **1** | What kind of analysis or other related work does the section most commonly deal with?  
e.g., disk and file imaging and analysis, event log analysis, network log analysis, email analysis. |
| **2** | What are the tools used to conduct the analysis and work in Q1 above? Explain the job of each one in brief. |
| **3** | (a) Does the section sometimes require additional evidence from external state, national or international sources?  
(b) If so, describe some typical cases where this is required. |
| **4** | (a) Does the section have standards and guidelines for the procedures of conducting the investigation, handling and preserving evidence, and prosecuting cases? If so, please identify these standards and guidelines.  
(b) Does the section have standards and guidelines for using the investigation tools? If so, please identify these standards and guidelines. |
| **5** | (a) What are some of the legal issues involved in cases dealt with by the section in uncovering evidence?  
e.g., privacy.  
(b) What are some of the practical issues in preserving evidence? |
<table>
<thead>
<tr>
<th>e.g., imaging, safe rooms.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(c) What are some of the technical issues in interpreting evidence?</td>
</tr>
<tr>
<td>e.g., encryption.</td>
</tr>
</tbody>
</table>

Thank you for participating in this questionnaire. As I mentioned earlier, if you have any inquiry or questions please do not hesitate to contact me, thanks again.
Appendix C.2: QPS – Interview Questions

QPS Participant 1

Interview Questions:

Part A

1. You mentioned that at present that there are certain countries from where criminal elements appear to be basing their illegal operations. Have the unit thought about any plan to overcome this matter internally, for example, filtering the Internet traffic from these countries? (See CQ - Q 2.11)

2. One of the issues that you mentioned is unsecured wireless networks for the general public. Are there any plans to increase awareness of the public about this issue and provide any assistance they may require? (See CQ - Q 2.11)

3. How may Internet Service Providers (ISPs) attempt to minimize risk of Denial of Service Attacks (DoS), for example, through controlling and filtering the suspicious incoming of Internet traffic to a specific location or site? (See CQ - Q 2.1)

4. During your period of work within this unit, have you come across interstate or international cases where it was difficult to initiate the investigations? If yes, please explain? (See CQ - Q 2.10 & Q 2.11)

5. Can you identify some of the IT training courses that are useful for computer crime investigators? (See CQ - Q 2.12 & Q 2.13)

Part B: General Questions:

6. Offences not committed in Qld are not recorded in the Qld crime reporting database. Is there any record of such crimes kept in a database or anywhere else in case the same suspects are involved in later crimes? (See CQ - Q 3.1.1a)

7. How can the unit manage the work with other jurisdictions when there are many suspects involved in the same crime and some of them reside in Qld and the others in other jurisdictions? Who will be responsible about running trials? (See CQ - Q 3.1.1a & Q 3.1.1b)

CQ: Completed Questionnaire  Q: Question
QPS Participant 2

Interview Questions:

Part A

1. Dumpster diving, mail theft, purchasing stolen personal information, phishing and domain spoofing are all examples of techniques used by criminals for identity theft. These techniques differ and their investigation will differ. Does this unit have a plan for the future to implement specific procedures to address each of the identity theft techniques? Please Explain? (See CQ - Q 2.4)

2. This question is about resources (e.g. equipments, budget, tools and information). What type of resources do you think are useful for identity crime investigators? (See CQ - Q 2.10)

Part B: General Questions:

3. Can you please explain some of the jurisdictional problems resulting from different international legislation? (See CQ - Q 3.2.3e)

4. How can the Identity Crime Unit tackle the challenge of cooperation with other organizations, private and public organizations, during the investigation processes? (See CQ - Q 2.10)

CQ: Completed Questionnaire Q: Question
QPS Participant 3

Interview Questions:

Part A

1. Dumpster diving, mail theft, purchasing stolen personal information, phishing and domain spoofing are all examples of techniques used by criminals for identity theft. These techniques differ and their investigation will differ. Does this unit have a plan for the future to implement specific procedures to address each of the identity theft techniques? Please Explain? (See CQ - Q 2.4)

2. This question is about resources (e.g. equipments, budget, tools and information). What type of resources do you think are useful for identity crime investigators? (See CQ - Q 2.10)

3. What type of expertise does the unit need? (See CQ - Q 2.10)

4. What type of training do you think is essential for identity crime investigators? (See CQ - Q 2.10)

Part B: General Questions:

5. Can you please explain some of the jurisdictional problems resulting from different international legislation? (See CQ – Q 2.10 & Q 3.2.3e)

6. How can the Identity Crime Unit tackle the challenge of cooperation with other organizations, private and public organizations, during the investigation processes? (See CQ - Q 2.10)

CQ: Completed Questionnaire Q: Question
QPS Participant 4

Interview Questions:

1. Nowadays, money laundering occurs across borders via wired or electronic transfer. What procedures are being used to investigate such electronic transfer cases? (See CQ - Q 2.4)

2. If a suspect is involved in a range of criminal offences such as identity crime, computer crime, and proceeds of crime, how does the Proceeds of Crime Unit manage the investigation with the other units that are involved in such cases? (See CQ - Q 2.8)

3. What type of training do you think is essential for upgrading and improving the skills of the money laundering investigators? (See CQ - Q 2.10 & Q 2.13)

4. Do you think that if the unit has a database to record all different types of techniques used for the purpose of money laundering, that it can help in combating this problem? (See CQ - Q 2.14)

5. You indicated in the questionnaire that there is no education for the public about the money laundering issue. However, one of the methods used by the criminals for concealing the proceeds of crime was using students as transfer managers. The idea was to transfer the money to a student’s account and then the student sends it to an overseas account. After that, the student receives a commission to done the transfer without knowing or caring about the origin of the transferred money. How can the unit help to protect the students from involving themselves in such criminal activities? (See CQ - Q 2.15)
QPS Participant 5

Interview Questions:

1. Nowadays, money laundering occurs across borders via wired or electronic transfer. What procedures are being used to investigate such electronic transfer cases? *(See CQ - Q 2.4)*

2. This question is about resources (e.g. equipments, budget, tools and information). What type of resources do you think are useful for proceeds of crime investigators? *(See CQ - Q 2.10)*

3. Do you think that if the unit has a database to record all different types of techniques used for the purpose of money laundering, that it can help in combating this problem? *(See CQ - Q 2.14)*

4. You indicated in the questionnaire that there is no education for the public about the money laundering issue. However, one of the methods used by the criminals for concealing the proceeds of crime was using students as transfer managers. The idea was to transfer the money to a student's account and then the student sends it to an overseas account. After that, the student receives a commission to done the transfer without knowing or caring about the origin of the transferred money. How can the unit help to protect the students from involving themselves in such criminal activities? *(See CQ - Q 2.15)*

5. You mentioned that the change in legislation to allow the seizure of offenders’ assets on behalf of victim could help bringing criminals to justice. Has there been any discussion by the unit to suggest that the mentioned change could help the money laundering investigators? If yes, please explain. *(See CQ - Q 3.3.5)*

6. What type of expertise does the unit need? *(See CQ - Q 2.11)*

CQ: Completed Questionnaire  Q: Question
QPS Participant 6

Interview Questions:

1. The role of the Internet generally, and networks specifically, in communications these days is very obvious. Are there any plans for conducting network log analysis and email analysis in the future criminal cases? If yes, please explain. (See CQ - Q 3.4.1)

2. X-ways Forensics, Forensic Toolkit (FTK) and SPADA are computer forensic tools used by the unit for conducting analyses. What are the reasons behind selecting those tools and what sort of cases are they especially suited to? (See CQ - Q 3.4.2)

3. When conducting computer forensic analysis, do you rely upon a collaboration of the tools? Please explain. (See CQ - Q 3.4.2)

4. You mentioned in the questionnaire that the unit does not have set standards or guidelines for conducting investigations and using the forensic tools. Could that influence the process of the investigation and reliability of the evidence? (See CQ - Q 3.4.4a & Q 3.4.4b)
QPS Participant 7

Interview Questions:

1. The role of the Internet generally, and networks specifically, in communications these days is very obvious. Are there any plans for conducting network log analysis and email analysis in the future criminal cases? If yes, please explain. (See CQ - Q 3.4.1)

2. X-ways Forensics and Forensic Toolkit (FTK) are computer forensic tools used by the unit for conducting analyses. What are the reasons behind selecting those tools and what sort of cases are they especially suited to? (See CQ - Q 3.4.2)

3. When conducting computer forensic analysis, do you rely upon a collaboration of the tools? Please explain. (See CQ - Q 3.4.2)

4. You mentioned in the questionnaire that the unit does not have set standards or guidelines for using the forensic tools. Could that influence the process of the investigation and reliability of the evidence? (See CQ - Q 3.4.4b)

5. This question is about resources (e.g. equipments, budget, tools and information). What type of resources do you think are useful for computer forensics investigators? (See CQ - Q 2.10)

6. What type of expertise does the unit need? (See CQ - Q 2.10)

7. What type of training do you think is essential for upgrading and improving the skills of the computer forensics investigators? (See CQ - Q 2.10 & Q 2.11 & Q 2.12)
Appendix C.3: ADP – Interview Questions

ADP Participants 1 and 2

Interview Questions:

1. Can you please identify the legislation under which investigation proceeds?
2. Is there a policy document which identifies how the section works? Please explain.
3. Do you have a computer forensics section or unit? Please explain.
4. If you don’t have a computer forensics lab, how can your section investigate computer crimes?
5. Usually, how long it takes to get the information you required from the ISP?
6. Have you been in any training?

ADP Participants 3 and 4

Interview Questions:

1. Can you please identify the legislation under which investigation proceeds?
2. Is there a policy document which identifies how the section works? Please explain.
3. Do you have a computer forensics section or unit? Please explain.
4. If you don’t have a computer forensics lab, how can your section investigate computer crimes?
5. Usually, how long it takes to get the information you required from the ISP?
6. If the offender is resides in another state, what are the procedures that the section follows?
7. Have you been in any training?
8. How does the section educate the public about the computer crimes?
Appendix D: Questionnaires and Interview Questions – Phase II

Appendix D.1: QPS – Questionnaire Questions

The Questionnaire Questions

Please answer as many questions as you can, and insert ‘not known’ or similar if you don’t know the answer to a question.

Please provide a response in the space allocated in the box under each question, or provide a reference to an available document which provides the response.

Introductory Questions

<table>
<thead>
<tr>
<th>Personal Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong> Interviewee contact details</td>
</tr>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Phone:</td>
</tr>
<tr>
<td>E-mail:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>2</strong> Organization details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization: Queensland Police Service</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>3</strong> Questionnaire date and location of completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location: Brisbane, QPS Headquarters</td>
</tr>
<tr>
<td>Date of completion: / /2008</td>
</tr>
</tbody>
</table>
2nd Questionnaire

The word ‘unit’ in this part means the unit where the interviewee actually operates.

‘Part A’ of the questionnaire should be answered by the following units: Computer Crime Investigation Unit; Identity Crime Unit and Proceeds of Crime Unit.

‘Part B’ of the questionnaire should be answered only by the Forensic Computer Examination Unit.

Part A – Common Questions

Question 1

1(a) If someone who resides in Qld used their computer to attack a computer system located in NSW, who is responsible for investigating the offence? (Tick any or all that are relevant)

☐ QPS
☐ NSW Police
☐ AFP
☐ Other:

1(b) In cases where there is a significant amount of money lost, are the responsibilities for the investigation still the same?

☐ Yes
☐ No

1(c) Do the procedures and responsibilities for the investigation differ according to different types of attacked computer or computer system (see immediately below) – if so, (i) please describe who is responsible for the investigation in each case, (ii) if there are differing procedures in each case, and (iii) how you prioritize between such cases:

- Domestic or SME business computer systems.
- Large business computer systems.
- State government department computer systems.
- Federal government department computer systems.
- Critical infrastructure.
**Question 2**

2(a) If someone who resides in NSW used their computer to attack a computer system located in Qld, who is responsible for investigating the offence? (Tick any or all that are relevant)
- QPS
- NSW Police
- AFP
- Other:

2(b) In cases where there is a significant amount of money lost, are the responsibilities for the investigation still the same?
- Yes
- No

2(c) Do the procedures and responsibilities for the investigation differ according to different types of attacked computer or computer system (see immediately below) – if so, (i) please describe who is responsible for the investigation in each case, (ii) if there are differing procedures in each case, and (iii) how you prioritize between such cases:
  - Domestic or SME business computer systems.
  - Large business computer systems.
  - State government department computer systems.
  - Federal government department computer systems.
  - Critical infrastructure.

**Question 3**

3(a) If a group of people who reside in Qld, NSW, and Victoria used their computers to attack multiple computers located in different states, who is responsible for investigating the offence? (Tick any or all that are relevant)
- QPS
- NSW Police
- Victoria Police
- AFP
- Other:

3(b) How will the investigation be run?

3(c) Who will be responsible for completing the final report? Please explain in detail.
3(d) Do the procedures and responsibilities for the investigation differ according to different types of attacked computer or computer system (see immediately below) – if so, (i) please describe who is responsible for the investigation in each case, (ii) if there are differing procedures in each case, and (iii) how you prioritize between such cases:
- Domestic or SME business computer systems.
- Large business computer systems.
- State government department computer systems.
- Federal government department computer systems.
- Critical infrastructure.

**Question 4**

4(a) If someone who resides in Qld used their computer to attack a computer system located in another country, who is responsible for investigating the offence? (Tick any or all that are relevant)
- QPS
- AFP
- Relevant country
- Other:

4(b) In cases where there is a significant amount of money lost, are the responsibilities for the investigation still the same?
- Yes
- No

4(c) Do the procedures and responsibilities for the investigation differ according to different types of attacked computer or computer system (see immediately below) – if so, (i) please describe who is responsible for the investigation in each case, (ii) if there are differing procedures in each case, and (iii) how you prioritize between such cases:
- Domestic or SME business computer systems.
- Large business computer systems.
- State government department computer systems.
- Federal government department computer systems.
- Critical infrastructure.
**Question 5**

5(a) If someone who resides in another country used their computer to attack a computer system located in Qld, who is responsible for investigating the offence? (Tick any or all that are relevant)
- QPS
- AFP
- Relevant country
- Other:

5(b) In cases where there is a significant amount of money lost, are the responsibilities for the investigation still the same?
- Yes
- No

5(c) Do the procedures and responsibilities for the investigation differ according to different types of attacked computer or computer system (see immediately below) – if so, (i) please describe who is responsible for the investigation in each case, (ii) if there differing procedures in each case, and (iii) how you prioritize between such cases:
  - Domestic or SME business computer systems.
  - Large business computer systems.
  - State government department computer systems.
  - Federal government department computer systems.
  - Critical infrastructure.

**Questions 6, 7 and 8**

Warrants and court orders provide law enforcement (LE) with authorization for search and seizure of properties and for interception of communications. The following questions 6, 7 and 8 below are in the context of computer crime investigations conducted by your unit.

**Question 6**

6(a) Who prepares and requests authorisation for warrants and court orders prior to conducting the search?

6(b) In the last 12 months, can you give an indication of how many of the cases you and/or your unit investigated required search warrants or a court order:
- All of them
- Most of them
Question 7
7(a) Who prepares and requests authorisation for warrants and court orders prior to conducting the seizure?

7(b) In the last 12 months, can you give an indication of how many of the cases you and/or your unit investigated required search warrants or a court order:
- All of them
- Most of them
- Half of them
- Minority of them
- None of them

Question 8
8(a) Who prepares and requests authorisation for warrants and court orders prior to conducting interception of communications?

8(b) In the last 12 months, can you give an indication of how many of the cases you and/or your unit investigated required search warrants or a court order:
- All of them
- Most of them
- Half of them
- Minority of them
- None of them

Question 9
9(a) Are there procedure documents that identify what tasks should be carried out during an investigation:
   i. For search
      - Yes
      - No
   ii. For seizure
Appendix D: Questionnaires and Interview Questions

9(b) Are there procedures documents that describe how tasks should be carried out during an investigation:
   iv. For search
      ☐ Yes
      ☐ No
   v. For seizure
      ☐ Yes
      ☐ No
   vi. For interception of communications
      ☐ Yes
      ☐ No

9(c) Are the documents in (a) and (b) above hard copy or online?
   ☐ Hard document
   ☐ Online document

9(d) If there are no such hard copies or online documents, how do new staff get to know the procedures?

Question 10

Investigating a computer crime could include the following stages: complaint or initial report of the alleged offence, initial investigation, substantial (possibly multi party or joint) investigation, prosecution, and final reporting.

10(a) To what extent do these stages actually exist in your investigations?

10(b) Please describe what the actual steps are in detail.
**Question 11**
For each of the computer crimes listed in the following table, list the numbers of each crime you investigated in the last 12 months and indicate in each case the number of successful outcomes.

<table>
<thead>
<tr>
<th>Type of Crime</th>
<th>Number of cases investigated</th>
<th>Number of successful outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malicious code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial of service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity theft</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harassment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Question 12**
What initiatives and activities does the unit use to deal with the following challenges and issues:

(a) training and resources,
(b) updating expertise,
(c) cooperation with other organizations or law enforcement,
(d) jurisdictional problems of CC,
(e) anonymity services and
(f) different international legislation relating to CC.

**Question 13**
The Council of Europe, G8 and Interpol indicated growing concern with regards to the threats of Botnets.

13(a) Has the unit been involved in investigating these types of crime? Please explain.

13(b) Are there specific procedures and techniques to investigate Botnets? Please explain.
Question 14
How does the Internet assist in investigating CC? (e.g. through providing information on new threats, availability of free forensic tools, etc.)

Question 15
15(a) Does your unit or any related unit in your police force have a role in educating the public regarding computer crimes such as ID theft, online auction fraud, malicious code, Phishing, credit card fraud and Botnets?

☐ Yes
☐ No

15(b) If yes, what is that role?

15(c) If yes to (a), what are the specific recommendations that are given to the public to prevent and minimize the risk from computer crimes?

Question 16
16(a) Does QPS have an estimation of CC statistics happening within their jurisdiction?

☐ Yes
☐ No

16(b) If yes, please explain?

The End of Part A of the Questionnaire
Part B – Computer Forensics

**Question 1**
For each of the following computer crimes listed in the table below, list the numbers of each crime you investigated in the last 12 months and indicate in each case the number of successful outcomes:

<table>
<thead>
<tr>
<th>Type of Crime</th>
<th>Number of cases investigated</th>
<th>Number of successful outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malicious code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial of service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity theft</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harassment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Question 2**
The Council of Europe, G8 and Interpol indicated growing concern with regards to the threats of Botnets.

2(a) Has the unit been involved in investigating these types of crime? Please explain.

2(b) Are there specific procedures and techniques to investigate Botnets? Please explain.

**Question 3**
How does the Internet assist in investigating CC? (e.g. through providing information on new threats, availability of free forensic tools, etc.)

**Question 4**
Computer Forensics investigators must ensure the validity and reliability of the digital evidence collected from an electronic device. For that, the investigators use
write blocker hardware and/or software to allow the acquisition of information on a digital device without altering or damaging the device’s contents. What type of write blockers does the unit use when taking an electronic image of digital devices? Please list them.

**Question 5**

What initiatives and activities does the unit use to deal with the following challenges and issues:

(a) training and resources,
(b) updating expertise,
(c) cooperation with other organizations or law enforcement,
(d) jurisdictional problems of CC,
(e) anonymity services and
(f) different international legislation relating to CC.

The End of Part B of the Questionnaire

The End of the Questionnaire

Thank You.
Appendix D.2: QPS – Interview Questions

QPS Participant 1

Interview Questions:

<table>
<thead>
<tr>
<th>Computer Crime Related Questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 You mentioned that only QPS, where the offender resides, is responsible for investigating the offence, not the state where the victim resides. Then you mentioned another case where the NSW Police, where the offender resides, and QPS where the victim resides, are both responsible for investigating the offence. Can you explain why the responsibilities are different in these two cases? <em>(See Q 1(a) &amp; Q 2(a))</em></td>
</tr>
<tr>
<td>2 You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the search. Can you explain why not all cases? <em>(See Q 6(b))</em></td>
</tr>
<tr>
<td>3 You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the seizure. Can you explain why not all cases? <em>(See Q 7(b))</em></td>
</tr>
<tr>
<td>4 Do you think the interception power is useful in investigating cyber crime offences? If yes, why? <em>(See Q 8(a))</em></td>
</tr>
<tr>
<td>5 Can you describe and explain what the actual steps of the investigation are? <em>(See Q 10(b))</em></td>
</tr>
<tr>
<td>6 Can you please identify the five most common computer crimes that are happening in your jurisdiction? Also, can you provide statistics about the five most common crimes investigated by your unit in the last 12 months and indicate in each case the number of successful outcomes? <em>(See Q 11)</em></td>
</tr>
<tr>
<td>7 You mentioned that QPS have statistics on CC statistics happening within their jurisdiction. Can you please provide these statistics? <em>(See Q 11)</em></td>
</tr>
<tr>
<td>8 Does your unit have a Standard Operating Procedures (SOPs) document that describes how the computer crime investigation should be carried out? If yes, can you please identify this document?</td>
</tr>
</tbody>
</table>
### QPS Participant 2

**Interview Questions:**

<table>
<thead>
<tr>
<th>Computer Crime Related Questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. You mentioned that the state where the offender resides is responsible for investigating the offence; and the state where the victim resides would provide assistance as required. Can you explain what type of assistance is needed from the state where the victim resides? <em>(See Q 1(a) &amp; Q 2(a))</em></td>
</tr>
<tr>
<td>2. You mentioned that QPS where the offender resides, and the other country where the victim resides, are both responsible for investigating the offence. Is there any role for the AFP during the investigation? <em>(See Q 4(a))</em></td>
</tr>
<tr>
<td>3. You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the search. Can you explain why not all cases? <em>(See Q 6(b))</em></td>
</tr>
<tr>
<td>4. You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the seizure. Can you explain why not all cases? <em>(See Q 7(b))</em></td>
</tr>
<tr>
<td>5. Do you think the interception power is useful in investigating cyber crime offences? If yes, why? <em>(See Q 8(a))</em></td>
</tr>
<tr>
<td>6. Can you describe and explain what the actual steps of the investigation are? <em>(See Q 10(b))</em></td>
</tr>
<tr>
<td>7. Can you please identify the five most common computer crimes that are happening in your jurisdiction? Also, can you provide statistics about the five most common crimes investigated by your unit in the last 12 months and indicate in each case the number of successful outcomes? <em>(See Q 11)</em></td>
</tr>
<tr>
<td>8. Does your unit have a Standard Operating Procedures (SOPs) document that describes how the computer crime investigation should be carried out? If yes, can you please identify this document?</td>
</tr>
</tbody>
</table>
QPS Participant 3

Interview Questions:

<table>
<thead>
<tr>
<th>Computer Crime Related Questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
</tbody>
</table>
QPS Participant 4

**Interview Questions:**

<table>
<thead>
<tr>
<th>Computer Crime Related Questions:</th>
</tr>
</thead>
</table>
| 1 You mentioned that the state where the offender resides and the state where the victim resides are both responsible for investigating the offence. Can you explain how the investigation will be run? Who will finalize the final report? *(See Q 1(a) & Q 2(a))*
| 2 You mentioned in cases where the offender resides in Queensland, and the victim resides in another country, then QPS, the relevant country and Interpol are all responsible for investigating the offence. Is there any role for the AFP during the investigation? *(See Q 4(a))*
| 3 You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the search. Can you explain why not all cases? *(See Q 6(b))*
| 4 You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the seizure. Can you explain why not all cases? *(See Q 7(b))*
| 5 Do you think the interception power is useful in investigating identity theft offences? If yes, why? *(See Q 8(a))*
| 6 Can you describe and explain what the actual steps of the investigation are? *(See Q 10(b))*
| 7 Can you provide statistics about the number of identity theft offences investigated by your unit in the last 12 months and the number of cases that have successful outcomes? *(See Q 11)*
| 8 How does the Internet assist in investigating identity theft offence? *(See Q 13)*
| 9 Does your unit or any related unit in your police force have a role in educating the public regarding identity theft? If yes, please explain that role. *(See Q 14(a) and 14(b))*
| 10 Does your unit have a Standard Operating Procedures (SOPs) document that describes how the identity crime investigation should be carried out? If yes, can you please identify this document?
QPS Participant 5

Interview Questions:

<table>
<thead>
<tr>
<th>Computer Crime Related Questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the search. Can you explain why not all cases? (See Q 1(b))</td>
</tr>
<tr>
<td>2. You mentioned that half of the cases your unit investigated required search warrants or a court order prior to conducting the seizure. Can you explain why not all cases? (See Q 2(b))</td>
</tr>
<tr>
<td>3. Do you think the interception power is useful in investigating proceeds of crime offences? If yes, why? (See Q 3(a))</td>
</tr>
<tr>
<td>4. Can you describe and explain what the actual steps of the investigation are? (See Q 5(b))</td>
</tr>
<tr>
<td>5. You indicated a number of proceeds of crime cases have been investigated. Were these cases investigated by you or by your unit? (See Q 6)</td>
</tr>
<tr>
<td>6. Does your unit have a Standard Operating Procedures (SOPs) document that describes how the proceeds of crime investigation should be carried out? If yes, can you please identify this document?</td>
</tr>
</tbody>
</table>
# QPS Participant 6

## Interview Questions:

<table>
<thead>
<tr>
<th>Computer Crime Related Questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the search. Can you explain why not all cases? <em>(See Q 1(b))</em></td>
</tr>
<tr>
<td>2. You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the seizure. Can you explain why not all cases? <em>(See Q 2(b))</em></td>
</tr>
<tr>
<td>3. You mentioned that the QPS Police have interception powers. Is that right? If yes, can you please explain? <em>(See Q 3(a))</em></td>
</tr>
<tr>
<td>4. Can you describe and explain what the actual steps of the investigation are? <em>(See Q 5(b))</em></td>
</tr>
<tr>
<td>5. You indicated a number of proceeds of crime cases have been investigated. Were these cases investigated by you or by your unit? <em>(See Q 6)</em></td>
</tr>
<tr>
<td>6. Does your unit have a Standard Operating Procedures (SOPs) document that describes how the proceeds of crime investigation should be carried out? If yes, can you please identify this document?</td>
</tr>
</tbody>
</table>
QPS Participant 7

Interview Questions:

<table>
<thead>
<tr>
<th>Computer Crime Related Questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Can you describe and explain what the actual steps of the investigation are?</td>
</tr>
<tr>
<td>2 You indicated a number of cases have been investigated. Were these cases investigated by you or by your unit? <em>(See Q 1)</em></td>
</tr>
<tr>
<td>3 Does your unit have a Standard Operating Procedures (SOPs) document that describes how the computer forensics investigation should be carried out? If yes, can you please identify this document?</td>
</tr>
</tbody>
</table>

QPS Participant 8

Interview Questions:

<table>
<thead>
<tr>
<th>Computer Crime Related Questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Can you describe and explain what the actual steps of the investigation are?</td>
</tr>
<tr>
<td>2 Can you please identify the five most common computer crimes that are happening in your jurisdiction? And also, can you provide statistics about the five most common crimes investigated by your unit in the last 12 months and indicate in each case the number of successful outcomes? <em>(See Q 1)</em></td>
</tr>
<tr>
<td>3 Does your unit have a Standard Operating Procedures (SOPs) document that describes how the computer forensics investigation should be carried out? If yes, can you please identify this document?</td>
</tr>
</tbody>
</table>
Appendix D.3: ADP – Questionnaire Questions

The Questionnaire Questions
Please answer as many questions as you can, and insert ‘not known’ or similar if you don’t know the answer to a question.

Please provide a response in the space allocated in the box under each question, or provide a reference to an available document which provides the response.

Introductory Questions

<table>
<thead>
<tr>
<th>Personal Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Interviewee contact details</td>
</tr>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Phone:</td>
</tr>
<tr>
<td>E-mail:</td>
</tr>
<tr>
<td>2 Organization details</td>
</tr>
<tr>
<td>Organization: Abu Dhabi Police</td>
</tr>
<tr>
<td>3 Questionnaire date and location of completion</td>
</tr>
<tr>
<td>Location:</td>
</tr>
<tr>
<td>Date of completion: / /2008</td>
</tr>
</tbody>
</table>

2nd Questionnaire

The word ‘unit’ in this part means the unit where the interviewee actually operates.

Question 1

1(a) If someone who resides in Abu Dhabi used their computer to attack a computer system located in Dubai, who is responsible for investigating the offence? (Tick any or all that are relevant)

- [ ] Abu Dhabi Police
- [ ] Dubai Police
1(b) In cases where there is a significant amount of money lost, are the responsibilities for the investigation still the same?

☐ Yes
☐ No

1(c) Do the procedures and responsibilities for the investigation differ according to different types of attacked computer or computer system (see immediately below) – if so, (i) please describe who is responsible for the investigation in each case, (ii) if there are differing procedures in each case, and (iii) how you prioritize between such cases:

- Domestic or SME business computer systems.
- Large business computer systems.
- State government department computer systems.
- Federal government department computer systems.
- Critical infrastructure.

Question 2

2(a) If someone who resides in Dubai used their computer to attack a computer system located in Abu Dhabi, who is responsible for investigating the offence? (Tick any or all that are relevant)

☐ Abu Dhabi Police
☐ Dubai Police
☐ Ministry of Interior
☐ Other:

2(b) In cases where there is a significant amount of money lost, are the responsibilities for the investigation still the same?

☐ Yes
☐ No

2(c) Do the procedures and responsibilities for the investigation differ according to different types of attacked computer or computer system (see immediately below) – if so, (i) please describe who is responsible for the investigation in each case, (ii) if there are differing procedures in each case, and (iii) how you prioritize between such cases:

- Domestic or SME business computer systems.
- Large business computer systems.
Appendix D: Questionnaires and Interview Questions - Phase II

- State government department computer systems.
- Federal government department computer systems.
- Critical infrastructure.

**Question 3**

3(a) If a group of people who reside in Abu Dhabi, Dubai, and Sharjah used their computers to attack multiple computers located in different states, who is responsible for investigating the offence? (Tick any or all that are relevant)

- [ ] Abu Dhabi Police
- [ ] Dubai Police
- [ ] Sharjah Police
- [ ] Ministry of Interior
- [ ] Other:

3(b) How will the investigation be run?

3(c) Who will be responsible for completing the final report? Please explain in detail.

3(d) Do the procedures and responsibilities for the investigation differ according to different types of attacked computer or computer system (see immediately below) – if so, (i) please describe who is responsible for the investigation in each case, (ii) if there are differing procedures in each case, and (iii) how you prioritize between such cases:

- Domestic or SME business computer systems.
- Large business computer systems.
- State government department computer systems.
- Federal government department computer systems.
- Critical infrastructure.

**Question 4**

4(a) If someone who resides in Abu Dhabi used their computer to attack a computer system located in another country, who is responsible for investigating the offence? (Tick any or all that are relevant)

- [ ] Abu Dhabi Police
- [ ] Ministry of Interior
4(b) In cases where there is a significant amount of money lost, are the responsibilities for the investigation still the same?

☐ Yes

☐ No

4(c) Do the procedures and responsibilities for the investigation differ according to different types of attacked computer or computer system (see immediately below) – if so, (i) please describe who is responsible for the investigation in each case, (ii) if there are differing procedures in each case, and (iii) how you prioritize between such cases:

- Domestic or SME business computer systems.
- Large business computer systems.
- State government department computer systems.
- Federal government department computer systems.
- Critical infrastructure.

---

Question 5

5(a) If someone who resides in another country used their computer to attack a computer system located in Abu Dhabi, who is responsible for investigating the offence? (Tick any or all that are relevant)

☐ Abu Dhabi Police

☐ Ministry of Interior

☐ Relevant country

☐ Other:

5(b) In cases where there is a significant amount of money lost, are the responsibilities for the investigation still the same?

☐ Yes

☐ No

5(c) Do the procedures and responsibilities for the investigation differ according to different types of attacked computer or computer system (see immediately below) – if so, (i) please describe who is responsible for the investigation in each case, (ii) if there differing procedures in each case, and (iii) how you prioritize between such cases:

- Domestic or SME business computer systems.
- Large business computer systems.
- State government department computer systems.
- Federal government department computer systems.
- Critical infrastructure.

Questions 6, 7 and 8

Warrants and court orders provide law enforcement (LE) with authorization for search and seizure of properties and for interception of communications. The following questions 6, 7 and 8 below are in the context of computer crime investigations conducted by your unit.

Question 6

6(a) Who prepares and requests authorisation for warrants and court orders prior to conducting the search?

6(b) In the last 12 months, can you give an indication of how many of the cases you and/or your unit investigated required search warrants or a court order:

- [ ] All of them
- [ ] Most of them
- [ ] Half of them
- [ ] Minority of them
- [ ] None of them

Question 7

7(a) Who prepares and requests authorisation for warrants and court orders prior to conducting the seizure?

7(b) In the last 12 months, can you give an indication of how many of the cases you and/or your unit investigated required search warrants or a court order:

- [ ] All of them
- [ ] Most of them
- [ ] Half of them
- [ ] Minority of them
- [ ] None of them

Question 8
8(a) Who prepares and requests authorisation for warrants and court orders prior to conducting interception of communications?

8(b) In the last 12 months, can you give an indication of how many of the cases you and/or your unit investigated required search warrants or a court order:

☐ All of them
☐ Most of them
☐ Half of them
☐ Minority of them
☐ None of them

Question 9

9(a) Are there procedure documents that identify what tasks should be carried out during an investigation:
   vii. For search
       ☐ Yes
       ☐ No
   viii. For seizure
       ☐ Yes
       ☐ No
   ix. For interception of communications
       ☐ Yes
       ☐ No

9(b) Are there procedures documents that describe how tasks should be carried out during an investigation:
   x. For search
      ☐ Yes
      ☐ No
   xi. For seizure
      ☐ Yes
      ☐ No
   xii. For interception of communications
      ☐ Yes
      ☐ No

9(c) Are the documents in (a) and (b) above hard copy or online?
9(d) If there are no such hard copies or online documents, how do new staff get to know the procedures?

**Question 10**

*Investigating a computer crime could include the following stages: complaint or initial report of the alleged offence, initial investigation, substantial (possibly multi party or joint) investigation, prosecution, and final reporting.*

10(a) To what extent do these stages actually exist in your investigations?

10(b) Please describe what the actual steps are in detail.

**Question 11**

For each of the computer crimes listed in the following table, list the numbers of each crime you investigated in the last 12 months and indicate in each case the number of successful outcomes.

<table>
<thead>
<tr>
<th>Type of Crime</th>
<th>Number of cases investigated</th>
<th>Number of successful outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malicious code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial of service attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity theft</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harassment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Question 12**

What initiatives and activities does the unit use to deal with the following challenges and issues:

- (g) training and resources,
- (h) updating expertise,
- (i) cooperation with other organizations or law enforcement,
- (j) jurisdictional problems of CC,
Appendices

(k) anonymity services and
(l) different international legislation relating to CC.

Question 13
The Council of Europe, G8 and Interpol indicated growing concern with regards to the threats of Botnets.

13(a) Has the unit been involved in investigating these types of crime? Please explain.

13(b) Are there specific procedures and techniques to investigate Botnets? Please explain.

Question 14
How does the Internet assist in investigating CC? (e.g. through providing information on new threats, availability of free forensic tools, etc.)

Question 15
15(a) Does your unit or any related unit in your police force have a role in educating the public regarding computer crimes such as ID theft, online auction fraud, malicious code, Phishing, credit card fraud and Botnets?

☐ Yes
☐ No

15(b) If yes, what is that role?

15(c) If yes to (a), what are the specific recommendations that are given to the public to prevent and minimize the risk from computer crimes?

Question 16
16(a) Does ADP have an estimation of CC statistics happening within their jurisdiction?

☐ Yes

☐ No

16(b) If yes, please explain?


---

**Question 17**

Computer Forensics investigators must ensure the validity and reliability of the digital evidence collected from an electronic device. For that, the investigators use write blocker hardware and/or software to allow the acquisition of information on a digital device without altering or damaging the device’s contents. What type of write blockers does the unit use when taking an electronic image of digital devices? Please list them.


---

**Question 18**

18(a) With regards to cooperative investigation between Computer Crime Unit (CCU) and other units within ADP, how does the CCU divide responsibilities during computer crime investigation?


18(b) What are these responsibilities?


---

**Question 19**

How does ADP receive and obtain information and reports with regards to transfers of proceeds of crime? (e.g. Central Bank, other financial institutions, other law enforcement agencies, undercover agents)


---

**Question 20**

Does the Forensic Evidence Unit (FEU) cooperate with the CCU? (e.g. by providing computer forensic examinations)


Question 21
21(a) With regards to sending staff to developed countries to gain experience regarding dealing with computer crimes, which are these developed countries?

21(b) Can you explain the reasons behind choosing these countries?

Question 22
If ADP does not have a computer forensic laboratory, then who has responsibility for:

22(a) Seizing computers and high-tech devices?

22(b) Analysing computers and high-tech devices?

Question 23
To what extent has the Cooperation Council for the States of Arabian Gulf (GCC) helped in countering cyber crime in the gulf region? Please describe the GCC efforts if any.

Thank You.
**Appendix D.4: ADP – Interview Questions**

**ADP Participant 1**

**Interview Questions:**

<table>
<thead>
<tr>
<th>Computer Crime Related Questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. You mentioned that ADP, where the offender resides, is not responsible for investigating the offence. Can you explain why ADP is not responsible? <em>(See Q 4(a))</em></td>
</tr>
<tr>
<td>2. You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the search. Can you explain why not all cases? <em>(See Q 6(b))</em></td>
</tr>
<tr>
<td>3. You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the seizure. Can you explain why not all cases? <em>(See Q 7(b))</em></td>
</tr>
<tr>
<td>4. Can you describe and explain what the actual steps of the investigation are?</td>
</tr>
<tr>
<td>5. You mentioned that eleven cases have been investigated. Does this number mean all cases you had investigated or does the number cover all crimes the unit had investigated? <em>(See Q 11)</em></td>
</tr>
<tr>
<td>6. Can you provide other types of cases that have happened in this state and investigated by your unit?</td>
</tr>
</tbody>
</table>
ADP Participant 2

Interview Questions:

**Computer Crime Related Questions:**

<table>
<thead>
<tr>
<th></th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>You mentioned that are eleven cases have been investigated, does this number means all cases you had investigated or the number cover all the unit had investigated? <em>(See Q 11)</em></td>
</tr>
<tr>
<td>2</td>
<td>If ADP does not have a computer forensics laboratory, then who has the responsibility for seizing and analyzing computers and high-tech devices? <em>(See Q 22(a))</em></td>
</tr>
<tr>
<td>3</td>
<td>Can you describe and explain what the actual steps of the investigation are?</td>
</tr>
</tbody>
</table>
ADP Participant 3

Interview Questions:

<table>
<thead>
<tr>
<th>Computer Crime Related Questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. You mentioned that the state where the victim reports the crime is responsible for investigating the offence? <em>(See Q 1(a))</em></td>
</tr>
<tr>
<td>2. You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the search. Can you explain why not all cases? <em>(See Q 6(b))</em></td>
</tr>
<tr>
<td>3. You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the seizure. Can you explain why not all cases? <em>(See Q 7(b))</em></td>
</tr>
<tr>
<td>4. You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting interception of communications. Can you explain why not all cases? <em>(See Q 8(b))</em></td>
</tr>
<tr>
<td>5. You mentioned that are three cases that have been investigated? Is that right? If not, how many cases have been investigated by the unit? <em>(See Q 11)</em></td>
</tr>
<tr>
<td>7. Can you provide other types of cases that have happened in this state and were investigated by your unit?</td>
</tr>
<tr>
<td><em>a. The offender in the UAE and the victim in another country (South Africa):</em></td>
</tr>
<tr>
<td><em>b. The offender in another country (Morocco) and the victim in the UAE:</em></td>
</tr>
</tbody>
</table>
# Interview Questions:

## Computer Crime Related Questions:

<table>
<thead>
<tr>
<th></th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>You mentioned that ADP where the offender resides is responsible for investigating the offence? <em>(See Q 1(a))</em></td>
</tr>
<tr>
<td>2</td>
<td>With regards to the crime where the offender resides in another country and the victim resides in Abu Dhabi, what is the role of the Ministry of Interior? <em>(See Q 5(a))</em></td>
</tr>
<tr>
<td>3</td>
<td>You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the search. Can you explain why not all cases? <em>(See Q 6(b))</em></td>
</tr>
<tr>
<td>4</td>
<td>You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the seizure. Can you explain why not all cases? <em>(See Q 7(b))</em></td>
</tr>
<tr>
<td>5</td>
<td>You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting interception of communications. Can you explain why not all cases? <em>(See Q 8(b))</em></td>
</tr>
<tr>
<td>6</td>
<td>You have not mentioned any number of the computer crimes that happened in your state and were investigated by ADP, can you explain why? <em>(See Q 11)</em></td>
</tr>
<tr>
<td>7</td>
<td>You mentioned that the unit ensures the validity and reliability of the digital evidence through the lab without any explanations, please explain? <em>(See Q 17)</em></td>
</tr>
<tr>
<td>8</td>
<td>Can you describe and explain what the actual steps of the investigation are?</td>
</tr>
</tbody>
</table>
### ADP Participant 5

**Interview Questions:**

<table>
<thead>
<tr>
<th>Computer Crime Related Questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. You mentioned that ADP, where the offender resides, is not responsible for investigating the offence. Can you explain why ADP is not responsible? <em>(See Q 4(a))</em></td>
</tr>
<tr>
<td>2. You mentioned that most cases your unit investigated required search warrants or a court order prior to conducting the seizure. Can you explain why not all cases? <em>(See Q 7(b))</em></td>
</tr>
<tr>
<td>3. Can you describe and explain what the actual steps of the investigation are?</td>
</tr>
</tbody>
</table>