A Comparative Study of Cybercrime in Criminal Law:

China, US, England, Singapore and the Council of Europe

Een vergelijkende studie naar de strafbaarstelling van cybercriminaliteit:

China, VS, Engeland, Singapore en de Raad van Europa

Proefschrift ter verkrijging van de graad van doctor aan de
Erasmus Universiteit Rotterdam op gezag van
de rector magnificus
Prof.dr. H.A.P. Pols
en volgens besluit van het College voor Promoties

De openbare verdediging zal plaatsvinden op
donderdag 15 december 2016 om 11.30 uur
door

Qianyun Wang
geboren te Shandong, China

Erasmus University Rotterdam

Promotiecommissie

Promotoren:	Prof.mr. P.A.M. Mevis
	Prof.dr. Y. Li
Overige leden:	Dr. C. van Noortwijk
	Prof.mr. H. de Doelder
	Prof.dr. T. Qi

Acknowledgements

‘Why do you pursue a PhD degree in a foreign country?’ is a question I am asked frequently. Audery Hepburn once said in Roman Holiday that ‘you can either travel or read, and either your body or soul must be on the way’. To me, the beauty of pursuing a PhD degree abroad is that both of my body and my soul are on the way. I once regret that I came to a strange county for a stressful task. But thanks to all those who have promoted, supported, and accompanied me, now I am glad I have come. I would like to express my gratitude to all of them.

First of all, sincere thanks to Prof. Yuwen Li and Prof. Paul Mevis, who have patiently and conscientiously supervised and promoted this research. They have guided me not only on how to conduct the PhD research, but also on the career in the field of law. Secondly, special thanks to my supervisor in China, Yu Zhigang, who has also stimulated and encouraged me during the whole project. Thirdly, the colleagues from Erasmus School of Law also provided their support. Many thanks to them, especially to the colleagues from the Criminal Law Department, including Mr. Joost Verbaan, Dr. Michiel von der Wolf, Dr. Joost Nan, Prof. F. W. Bleichtodt, Prof. Hans de Doelder, Dr. Jaap van de Hulst, Dr. John Blad, Dr. Jolande uit Beijerse, Dr. Sanne Struijk, and Mr. Maradona. Fourthly, thanks to Ms. Marianne Breijer-de Man and Ms. Simone Rettig for arranging all the administration issues and helping with the paperwork. Fifthly, thanks also go to the friends in China Law Centre and Erasmus Graduate School of Law. The significance of their suggestions and comments on my thesis are beyond words. If not with them, I may not have succeeded. Thanks to Pei Wei, Ma Yun, Yuan Bo, Feng Yang, Liu Shuo, Yuhan, Xin Wen, Xun Xiao, Yixin, Qiqi, Hu Yi and Bian Cheng; and Eelco, Liselotte, Stefan, Erlis, Jing, Thomas, Renata, Randolf, Arien, and Piotr.

In the end, this book is a gift to my parents, Wang Xuemin and Tang Yufang, and my fiancée Tian Li. Thank you for your understanding and support.

Wang Qianyun

September 2016

Table of Contents

Acknowledgements I

Abbreviations XI

List of Main Laws and Official Documents XIII

Chapter 1 Introduction 1

1.1 Research Background 1

1.2 Research Subject 4

1.2.1 The concept of cybercrime 4

1.2.1.1 Computer crime and cybercrime 5

1.2.1.2 Computer crime and computer-related crime 7

1.2.1.3 Cybercrime and economic crime 8

1.2.1.4 Cybercrime and intellectual property infringement 9

1.2.2 Classification of cybercrime 9

1.3 Problem Statement: the scale of cyber wrongdoing and the challenges it poses to criminal law 11

1.3.1 The scale of cyber wrongdoing 11

1.3.2 The challenges to criminal law 17

1.4 Research Question and Research Structure 23

1.4.1 Research question 23

1.4.2 Research structure 24

1.5 Research Methods 25

1.5.1 Doctrinal research 25

1.5.2 Comparative Study 26

1.5.2.1 China 26

1.5.2.2 The Council of Europe 26

1.5.2.3 The United States and England 27

1.5.2.4 Singapore 28

Chapter 2 The Cybercrime Legislation in China 29

2.1 Introduction 29

2.2 An Overview of the Regulatory System Regarding Cyber Wrongdoing 29

2.2.1 Criminal Law, Amendments to the Criminal Law, and Decisions 32

2.2.2 Administrative regulations and departmental rules 34

2.2.2.1 Administrative regulations 35

2.2.2.2 Departmental rules 37

2.2.3 Judicial Interpretation and cases 38

2.2.3.1 Judicial Interpretation 38

2.2.3.2 Cases 40

2.3 Historical Review of the Cybercrime Legislation in China 41

2.3.1 Pre 1997: a vacuum in cybercrime legislation 42

2.3.2 From 1997 to 2009: the criminal provisions against cybercrime and their application 44

2.3.3 After 2009: amendments and expansions 50

2.4 Current Legislation on Cybercrime 53

2.4.1 Illegal access to computer 53

2.4.1.1 Illegal access to the listed computer information system 53

2.4.1.2 Illegal changing of data stored on a computer information system and illegal control over a computer information system 55

2.4.1.3 Providing special tools for illegal access, illegal obtaining of data and illegal control over computers 55

2.4.2 Computer interference 57

2.4.3 Criminal liability of network service providers 58

2.4.4 Traditional crimes facilitated by computer 59

2.4.5 Illegal use of the information network 60

2.4.6 Ancillary liability – aiding and abetting 60

2.4.7 Jurisdiction....61
2.5 The Scope of Cybercrime....64
2.5.1 Three opinions on determining cybercrime....64
2.5.2 The effect of different opinions in judicial practice....66
2.6 Summary....68
Chapter 3 The Convention on Cybercrime of the Council of Europe....71
3.1 Introduction....71
3.2 Historical Review of the Endeavours by the Council of Europe....71
3.2.1 Historical review of the CoE efforts against cybercrime....72
3.2.1.1 In the 1970s**:** tackling 'computer crime' with the economic crime legislation....72
3.2.1.2 In the 1980s: negotiating and preparing for the substantive criminal law on 'computer-related crime'....73
3.2.1.3 In the 1990s: harmonising the procedural criminal law....74
3.2.2 Main discussions behind the CoC....75
3.2.3 The Main Waves of Domestic Cybercrime Legislation....79
3.3 The Offences under the Convention on Cybercrime....81
3.3.1 Terms used in the CoC....84
3.3.2 Offences against the security of computer....86
3.3.2.1 Illegal Access....86
3.3.2.2 Illegal interception....88
3.3.2.3 Data interference....89
3.3.2.4 System interference....90
3.3.2.5 Misuse of devices....91
3.3.3 Traditional crimes facilitated by computer....93
3.3.3.1 Computer-related offences....93
3.3.3.2 Offences related to child-pornography....95

3.3.3.3 Offences related to infringements of copyright and related rights 95
3.3.4 Jurisdiction.....96
3.4 Summary 97
Chapter 4 The Cybercrime Legislation in the United States 99
4.1 Introduction 99
4.2 Historical Review of the Cybercrime Legislation in the US.....99
4.2.1 The evolution of the Computer Fraud and Abuse Act.....99
4.2.1.1 Pre 1984: initial efforts in drafting a cybercrime legislation 101
4.2.1.2 From 1984 to 1986: the first legislation focusing on cybercrime.....105
4.2.1.3 After 1986: expansions and amendments 106
4.2.2 Competing arguments behind the legislation 112
4.2.2.1 Arguments against a cyber-specific legislation 113
4.2.2.2 Arguments for a cyber-specific legislation 115
4.3 Current Legislation on Cybercrime.....118
4.3.1 Offences against the security of computer 118
4.3.1.1 Access offences.....118
4.3.1.2 Impairment of computer 127
4.3.1.3 Misuse of devices.....129
4.3.1.4 Interception of communication and data.....131
4.3.2 Traditional crimes facilitated by computer.....132
4.3.2.1 Computer facilitated fraud and forgery.....132
4.3.2.2 Offences related to child-pornography 134
4.3.2.3 Offences related to infringements of copyright and related rights 135
4.3.3 Jurisdiction.....137
4.4 The Scope of Cybercrime and the Attitude towards the CoC in the US.....138
4.4.1 The scope of cybercrime.....138

4.4.2 The American attitude towards the Convention on Cybercrime 140
4.5 Summary 143
Chapter 5 The Cybercrime Legislation in England 147
5.1 Introduction 147
5.2 Historical Review of the Cybercrime Legislation in England 148
5.2.1 The evolution of Computer Misuse Act 148
5.2.1.1 Pre 1990: initial attempts to use traditional criminal law tackling computer misuses 148
5.2.1.2 From 1990 to 2006: the first legislation on computer misuse 155
5.2.1.3 After 2006: updates and expansions 155
5.2.2 Competing arguments behind the criminalisation of mere hacking 158
5.2.2.1 Arguments for criminalising mere hacking 158
5.2.2.2 Arguments against criminalising mere hacking 159
5.3 Current Legislation on Cybercrime 160
5.3.1 Offences against the security of computer 160
5.3.1.1 Access offences 161
5.3.1.2 Impairment of data 164
5.3.1.3 Interception of data 166
5.3.1.4 Misuse of devices 169
5.3.1.5 Unauthorised acts causing, or creating risk of, serious damage 171
5.3.2 Traditional crimes facilitated by computer 172
5.3.2.1 Computer facilitated fraud and forgery 172
5.3.2.2 Offences related to child-pornography 173
5.3.2.3 Offences related to infringemtnd of copyright and related rights 174
5.3.3 Jurisdiction 175
5.4 The Scope of Cybercrime 176
5.5 Summary 178

Chapter 6 The Cybercrime Legislation in Singapore 183

6.1 Introduction 183

6.2 Historical Review of the Cybercrime Legislation in Singapore 183

6.2.1 From 1993 to 1996: the first computer specific legislation 184

6.2.2 After 1993: expansions and amendments 185

6.2.2.1 The Evidence (Amendment) Act 1996: an effort to enhance administrative powers 185

6.2.2.2 The Computer Misuse (Amendment) Act 1998: introductions of new offences and increases of penalties 186

6.2.2.3 The Computer Misuse (Amendment) Act 2003: an expansion of enforcement powers 189

6.2.2.4 The Computer Misuse (Amendment) Act 2013: further expansions of enforcement powers 189

6.3 Current Legislation on Cybercrime 191

6.3.1 Offences against the security of computer 191

6.3.1.1 Access offence 191

6.3.1.2 Data interference and system interference 198

6.3.1.3 Misuse of devices 199

6.3.1.4 Unauthorised use or interception of computer service 200

6.3.2 Traditional crimes facilitated by computers 203

6.3.2.1 Computer facilitated fraud and forgery 203

6.3.2.2 Offences related to child-pornography 205

6.3.2.3 Offences related to infringements of copyright and related rights 206

6.3.3 Jurisdiction 207

6.4 The Scope of Cybercrime and the Enforcement Measures 209

6.4.1 The scope of cybercrime 210

6.4.2 The enforcement measures under the Computer Misuse Act 212

6.5 Summary 217

Chapter 7 Comparison, Conclusion and Recommendation 219

7.1 Introduction 219

7.2 Comparison 220

7.2.1 On-going legislative process in expanding cybercrime legislation 220

7.2.1.1 Specific cybercrime Act v. general criminal law 220

7.2.1.2 The origin of cybercrime legislation: the inadequacy of traditional criminal provisions and the consequent necessity for new cybercrime legislation 222

7.2.1.3 Key amendments to cybercrime legislations: an expanding process 227

7.2.2 National security as the main motivation behind the expanding process 232

7.2.3 The capacity of judges on adjudicating cybercrime cases 235

7.2.4 Unsolved issue of defining cybercrime 238

7.2.5 Elements steering the scope of cybercrime 245

7.2.5.1 The concept of computer 245

7.2.5.2 Unauthorised access, exceeds authorised access, or access violating States' regulations 251

7.2.5.3 'Fault element' of cybercrime: intention, knowledge and recklessness 257

7.2.5.4 Examining the scope of cybercrime 258

7.2.6 The function of computer and the security of data: two different legal interests 261

7.2.7 Inadequacy of the existing jurisdiction principles over cybercrime 265

7.3 Conclusion 269

7.3.1 The necessity of cyber-specific legislation 269

7.3.2 The advantages and disadvantages of legislative approaches in the selected legal regimes 270

7.3.3 The time for fresh thinking on the jurisdiction issue 275

7.3.4 The Convention on Cybercrime as an international legal standard against cybercrime 276

7.4 Recommendation to China 277

7.5 Final Remarks 282
Appendices 283
Appendix I Relevant Legal Provisions of the Chapter on China 283
Appendix II Relevant Legal Provisions of the Chapter on the Council of Europe 293
Appendix III Relevant Legal Provisions of the Chapter on the United States 305
Appendix IV Relevant Legal Provisions of the Chapter on England 319
Appendix V Relevant Legal Provisions of the Chapter on Singapore 329
Bibliography 345
Summary 351

Abbreviations

CII	Critical Information Infrastructure
CL	Criminal Law
CNNIC	China Internet Network Information Centre
CoC	Convention on Cybercrime
CoE	Council of Europe
EAPIG	(England) All Party Internet Group
ECDA	(England) Criminal Damage Act
ECDPA	(England) Copyright, Designs and Patents Act
ECMA	(England) Computer Misuse Act
EFA	(England) Fraud Act
EFCA	(England) Forgery and Counterfeiting Act
EPJA	(England) Police and Justice Act 2006
ERCoC	Explanatory Report of the Convention on Cybercrime
ERIPA	(England) Regulation of Investigatory Powers Act
ESCA	(England) Serious Crime Act
ETA	(England) Theft Act
FBI	(US) Federal Bureau of Investigation
GPS	Global positioning system
ISP	Internet Service Provider
MP	Member of Parliament
NPC	(China) National People's Congress
OECD	Organisation for Economic Co-operation and Development
PC	Penal Code
SC	(China) State Council
SCMA	(Singapore) Computer Misuse Act
SCMAA	(Singapore) Computer Misuse (Amendment) Act
SCNPC	(China) Standing Committee of the National People's Congress
SPC	(China) Supreme People's Court
SPP	(China) Supreme People's Procuratorate
USBFCSPA	(US) Bill of the Federal Computer Systems Protection Act
USCFAA	(US) Computer and Fraud Abuse Act
USITERA	(US) Identity Theft Enforcement and Restitution Act
USNIIPA	(US) National Information Infrastructure Protection Act
USPA	(US) Patriot Act
USPRA	(US) Pen Register Act
USSCA	(US) Stored Communications Act
USWA	(US) Wiretap Act

List of Main Laws and Official Documents

China

1979 年中华人民共和国人民法院组织法 (Organic Law of People's Court 1997) (2006 revised)

1982 年中华人民共和国宪法 (Constitution 1982) (2004 revised)

1994 年中华人民共和国计算机信息系统安全保护条例，中华人民共和国国务院令 1 4 7 号 (Safety and Protection Regulations for Computer Information Systems 1994, Decree No. 147 of the State Council) (2011 revised)

1997 年计算机信息网络国际联网安全保护管理办法，中华人民共和国公安部令 33 号 (Measures for Security Protection in the Administration of the International Networking of Computer Information Networks 1997, Decree No. 33 of the Ministry of Public Security) (2011 revised)

1997 年中华人民共和国刑法 (Criminal Law 1997) (2015 revised)

2000 年中华人民共和国立法法 (Legislation Law 2000) (2015 revised)

2004 年最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释（二），法释[2010]3 号 (Interpretations (II) of the Supreme People's Court and the Supreme People's Procuratorate on the Application of Law in Handling Criminal Cases about Producing, Reproducing, Publishing, Selling and Disseminating Pornographic Electronic Information via the Internet, Mobile Communication Terminals and Sound Message Stations**,** Fa Shi [2010] No. 3)

2006 年中华人民共和国治安管理处罚法 (Public Security Administration Punishments Law 2006) (2013 revised)

2008 年中华人民共和国计算机信息网络国际联网管理暂行规定，国务院令第 195 号 **(**Interim Regulations on the Management of International Networking of Computer Information Network 1996, Decree No. 195 of the State Council**)**

2009 年中华人民共和国刑法修正案（七）(Amendment (VII) to the Criminal Law 2009)

2009 年最高人民法院关于裁判文书引用法律、法规等规范性法律文件的规定，法释[2009] 14 号 (Provisions of the Supreme People's Court on the Citation of Such Normative Legal Documents as Laws and Regulations in the Judgements, Fa Shi [2009] No. 14)

2010 年最高人民法院印发《关于案例指导工作的规定》通知，法发[2010] 51 号 (Preamble of Notice of the Supreme People's Court on Issuing the Provisions on Case Guidance, Fa Fa [2010] No. 51)

2011 年最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释，法释[2011] 19 号 **(**Interpretations of the Supreme People's Court and the Supreme People's Procuratorate on the Application of Law in Handling Criminal Cases about Endangering the Security of Computer Information Systems, Fa Shi [2011] No. 19**)**

2012 年全国人大常委会关于加强网络信息保护的决定，2012 年 12 月 28 日第十一届全国人民代表大会常务委员会第三十次会议通过 (Decisions of the Standing Committee of the National People's Congress Regarding the Strengthening of Network Information Protection 2012)

2012 年最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定，法[2012]20 号 (Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks, Fa Shi [2012] No. 20)

2013 年高人民法院、最高人民检察院关于办理盗窃刑事案件适用法律若干问题的解释，法释[2013] 8 号 (Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Theft, Fa Shi [2013] No. 8)

2013 年最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释，法释[2013] 21 号 (Interpretations of the Supreme People's Court and the Supreme People's Procuratorate on the Application of Law in the Handling of Defamation Cases through the Use of Information Networks, Fa Shi [2013] No. 21)

2015 年中华人民共和国刑法修正案（九） (Amendment (IX) to the Criminal Law 2015)

United States

17 U.S.C. § 506 Copyrights Criminal Offences

18 U.S.C. § 1028 Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information

18 U.S.C. § 1029 Fraud and Related Activity In Connection With Access Devices

18 U.S.C. § 1030 Fraud and Related Activity in Connection with Computers

18 U.S.C. § 1343 Fraud by Wire, Radio, or Television

18 U.S.C. § 2251 Sexual Exploitation of Children

18 U.S.C. § 2252 Certain Activities Relating to Material Involving the Sexual Exploitation of Minors

18 U.S.C. § 2256 Definitions for Chapter

18 U.S.C. § 2260 Production of Sexually Explicit Depictions of A Minor for Importation into the United States

18 U.S.C. § 2511 Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited

18 U.S.C. § 2701 Unlawful Access to Stored Communications

Internet Crime Report 2013, Internet Crime Complaint Centre, Federal Bureau of Investigator

England

Theft Act 1968

Criminal Damage Act 1971

Protection of Children Act 1978

Forgery and Counterfeiting Act 1981

Copyright, Designs and Patents Act 1988

Computer Misuse working Paper No. 110, the Law Commission

Computer Misuse No. 186 (1989), the Law Commission

Computer Misuse Act 1990

Data Protection Act 1998

Criminal Justice and Court Service Act 2000

Regulation of Investigatory Powers Act 2000

Identity Cards Act 2006

Fraud Act 2006

Police and Justice Act 2006

Serious Crime Act 2015

Singapore

Internal Security Act (Chapter 143) 1987

Computer Misuse Act (Chapter 50A) 1993

Evidence (Amendment) Act 1996

Computer Misuse (Amendment) Act 1998

Films Act (Chapter 107) 1998

Undesirable Publication Act (Chapter 338) 1998

Computer Misuse (Amendment) Act 2003

Copyright Act (Chapter 63) 2006

Penal Code (Chapter 224) 2008

Personal Data Protection Act 2012

Judicial Proceedings (Regulation of Publication) Act (Chapter 149) 2013

Council of Europe

Recommendation No. R (81) 12, the Committee of Ministers to Member States on Economic Crime, adopted by the Committee of Ministers

Recommendation No. R (89) 9 on Computer-related Crime, the European Committee on Crime Problems

Recommendation No. R (95) 13, the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology, adopted by the Committee of Ministers

Convention on Cybercrime 2001

Explanatory Report of Convention on Cybercrime 2001

Others

International Covenant on Civil and Political Rights

Canadian Criminal Code 1985 Rev. Ed.

Computer-Related Criminality: Analysis of Legal Policy, 1986, Organization for Economic Co-operation and Development (OECD)

Chapter 1 Introduction

1.1 Research Background

Developments in information and communication technology and digital computing devices have dramatically changed the ways in which people live and communicate. Taking China as an example: a survey conducted by the Chinese Internet Network Information Centre (hereafter the CNNIC) reveals that, by June 2015, 668 million Chinese citizens had a connection to the Internet; that more than 600 million of these used the Internet to communicate with others, more than 500 million used the Internet to search for news, and around 400 million made online purchases. This survey also revealed that other online services, such as personal blogs, online video and online games have enormous numbers of users as well.[1]

However, new developments in information technology also provide new opportunities for offenders, a problem which already challenges, and will continue to challenge, the criminal law system. Firstly, new offences targeting computers and data have become increasingly common: hackings launched between the United States and China have attracted attention worldwide.[2] Secondly, traditional offences are also stimulated by the new opportunities.[3] As has been observed, 'the magic of digital cameras and the sharing of photos on the Internet is exploited by child pornographers; the convenience of electronic banking and online sales provides fertile ground for fraud; electronic communications such as email and SMS may be used to stalk and harass.'[4]

What makes the situation even worse is that the frequently reported cyber wrongdoings have not attracted enough attention among the 'netizens', as the community of regular Internet users is sometimes called. In 2012, the CNNIC conducted a survey on the issue of network

[1] CNNIC, '第 36 次中国互联网发展状况统计报告（2015 年 7 月）' (The 36th Report on China Information Network Development (July 2015)), available at http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201507/P020150723549500667087.pdf. Last visited November 2015.

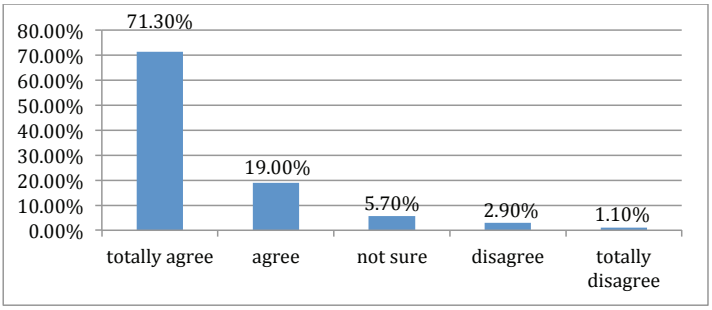
[2] See e.g. Rupert Cornwell, 'US Declares Cyber War on China: Chinese Military Hackers Charged with Trying to Steal Secrets from Companies Including Nuclear Energy Firm', *Independent*, 19 May 2014, available at http://www.independent.co.uk/life-style/gadgets-and-tech/us-charges-chinese-military-hackers-with-cyber-espionage-bid-to-gain-advantage-in-nuclear-power-9397661.html. Last visited February 2016. See also Mark Thompson, 'Continued Hacking Highlights U.S-Chinese Cyberwar Worries', *Time*, 5 June 2015, available at http://time.com/3910897/office-personnel-management-hack/. Last visited February 2016.

[3] See e.g. Tom Grubb, 'The Five A's that Make Cybercrime So Attractive', *Securityweek*, 26 April 2010, available at http://www.securityweek.com/five-a%E2%80%99s-make-cybercrime-so-attractive. Last visited February 2016. See also Noah Rayman, 'The World's Top 5 Cybercrime Hotspots', *Time*, 7 August 2014, available at http://time.com/3087768/the-worlds-5-cybercrime-hotspots/. Last visited February 2016.

[4] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 3.

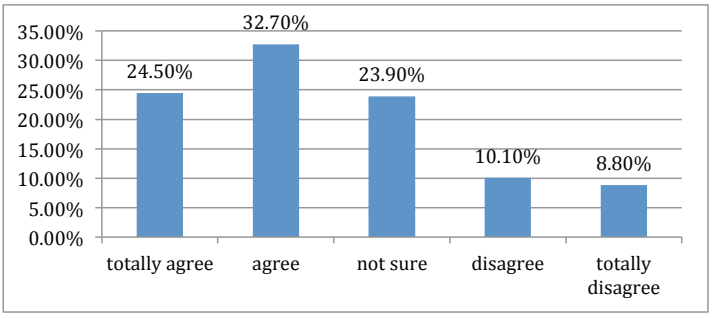
security. This survey showed that although more than 90% of netizens acknowledged the importance of paying attention to the online security, only 15.1% of them would be likely to file a complaint either to the authorities[5] or to service providers[6] if they encountered cyber infringements.[7]

Figure 1.1: Opinions on 'it is important to pay attention to information security'



(Source: CNNIC)

Figure 1.2: Opinions on 'if my digital devices suffer incidents, I will suffer subsequently'



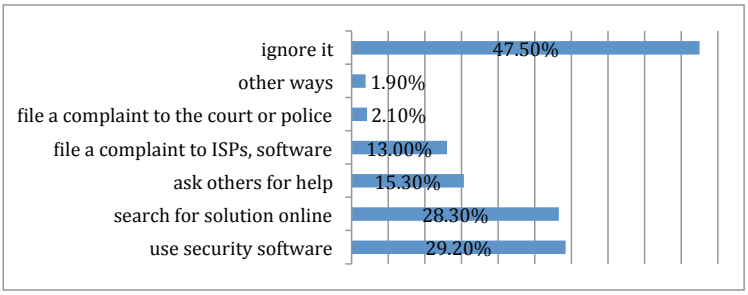
(Source: CNNIC)

[5] 'Authorities' here includes the court and the police. As demonstrated in Figure 1.3, only 2.1% of netizens will file a complaint to the court or the police if they encounter cyber infringements.

[6] 'Service providers' here includes the Internet service provider, software publisher and website administrator. As demonstrated in Figure 1.3, 13% of netizens will file a complaint to Internet service providers, software publishers or website administrators if they encounter cyber infringements.

[7] CNNIC, 'The Statistical Report on Information Security of Chinese Netizens 2012', available at http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/mtbg/201212/P020121227486012736156.pdf. Last visited July 2013.

Figure 1.3: Ways of handling information security infringements by individuals



(Source: CNNIC)

In this context, computers and data are vulnerable to crime, especially with the introduction of technology that also connects computers, televisions, phones and other household appliances to the information network.[8] Statistics collected by the Chinese Internet Crime Report Centre *(中国网络违法犯罪举报网站)* show that in 2014, it received more than 367,489 complaints of incidents from netizens, 110,320 of which are suspected to be illegal, including 40,546 complaints about online fraud, 36,654 complaints about online pornography, and 2,818 complaints about the impairment of computers.[9] These statistics may not seem very remarkable, but taking into consideration the fact that only 15.1% of netizens will file a complaint, as has been shown by the previously mentioned 2012 survey,[10] the actual number of victims may be seven times that of the number of complaints received.

Nor do other jurisdictions appear to be doing well when it comes to regulating cyber wrongdoing. The Internet Crime Complaint Centre of the US Federal Bureau of Investigation (hereafter the FBI) received 269,422 complaints from netizens in 2014, resulting in a reported

[8] Yu Zhigang, '三网融合背景下刑事立法的调整方向' (The Direction of the Criminal Law Legislation in the Context of the Combination of Internet, Telecommunication Network and Television Network), *Faxue Luntan* (Legal Forum), 7(2012): 5-12, p. 5.

[9] '2014 年举报受理处置情况' (Annual Report of Received Complaints 2014), *网络违法犯罪举报网站* (Internet Crime Report Centre), 19 January 2015, available at http://www.cyberpolice.cn/wfjb/html/xxgg/20150119/1085.shtml. Last visited November 2015.

[10] CNNIC, 'The Statistical Report on Information Security of Chinese Netizens 2012', available at http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/mtbg/201212/P020121227486012736156.pdf. Last visited February 2016.

financial loss of $ 800,492,073 for the victims.[11] In addition, as reported, over 600,000 Facebook accounts are hacked into every single day,[12] and 30 million new malwares were created in 2013, amounting to some 82,000 each day.[13]

Given the netizens' tendency to overlook the cyber security issue, coupled with the huge number of cyber infringements, legislative measures to regulate cyber wrongdoing have become a hot topic. This research examines how the selected legal regimes have adapted their criminal laws to deal with cybercrime. The aim of this research is to *analyse the legislative approaches taken by the selected legal regimes when adapting their substantive criminal law*, and, *to explore solutions to cybercrime through a comparison of these approaches.*

1.2 Research Subject

> 'The range of technology-enabled crime is always evolving, both as a function of technological change and in terms of social interaction with new technologies.'[14]

1.2.1 The concept of cybercrime

This research adopts two interchangeable terms 'cybercrime' and 'computer crime' to refer to its subject matter. The concepts of these two terms and some of the other main terms used to describe the subject of this research are discussed in the following, as well as the reasons for choosing these two. Afterwards, their relationships to two terms 'economic crime' and 'intellectual property infringement', which on some occasions may overlap with the subject of this research, are examined.

---

[11] Internet Crime Complaint Centre, Federal Bureau of Investigation, the United States, '2014 Internet Crime Report', available at https://www.fbi.gov/news/news_blog/2014-ic3-annual-report, last visited February 2016.

[12] See e.g. Emma Barnett, 'Hackers Go After Facebook Sites 600,000 Times Every Day', *The Telegraph*, 29 October 2011, available at http://www.telegraph.co.uk/technology/facebook/8856417/Hackers-go-after-Facebook-sites-600000-times-every-day.html. Last visited February 2016.

[13] Tony Bradley, 'Report: Average of 82,000 New Malware Threats Per Day in 2013', *PCWorld*, 18 May 2014, available at http://www.pcworld.com/article/2109210/report-average-of-82-000-new-malware-threats-per-day-in-2013.html. Last visited February 2016.

[14] G. Urbas and K. R. Choo, Resource Materials on Technology-enabled Crime, *Technical and Background Paper No. 28 (AIC, 2008)*, p. 5. In this paper 'technology-enabled crime' are the crimes that require information and communication technology for their commission. It roughly refers to the subject of this research – cybercrime.

1.2.1.1 Computer crime and cybercrime

From the initial terms such as 'computer crime',[15] 'computer-related crime',[16] and 'crime by computer',[17] to more digital concepts, such as 'high-technology crime',[18] 'technologically enabled crime',[19] 'virtual crime',[20] and 'digital crime',[21] a dozen or so terms have been used. Apart from these terms, to emphasise the involvement of the Internet, 'cybercrime'[22] (or 'cyber crime'/'cyber-crime') and 'network crime'[23] have also been deployed.

It can be observed that the initial terms focus on the 'computer'. Among them, 'computer crime' can, roughly speaking, be regarded as those crimes in which a computer 'plays as the target, the tool or incidental'.[24] 'Computer-related crime' is defined as that which 'entails the use of digital technologies in the commission of the offence; is directed at computing and communications technologies themselves; or involves the incidental use of computers with respect to the commission of other crimes'.[25] The term 'crime by computer' refers to those crimes committed by using a computer, to which the group that 'entails the use of digital

[15] See e.g. Donn B. Parker, *Fighting Computer Crime*, New York: Charles Scribner's Sons, 1983.

[16] See e.g. United Nations Office on Drugs and Crime, 'Computer-Related Crime', *The 11th United Nations Congress on Crime Prevention and Criminal Justice*, 18-25 April 2005, Bangkok, Thailand, available at http://www.unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf. Last visited November 2015.

[17] See e.g. Richard C. Hollinger, 'Crime by Computer: Correlations of Software Piracy and Unauthorised Account Access', *Security Journal,* vol. 4 1(1993): 2-12.

[18] See e.g. Larry E. Coutorie, 'The Future of High-Technology Crime: A Parallel Delphi Study', *Journal of Criminal Justice*, vol. 23 1(1995): 13-27.

[19] See e.g. Sarah Gordon, 'Technologically Enabled Crime: Shifting Paradigms for the Year 2000', *Computer and Security*, vol. 14 5(1995): 391-402. The term 'technologically enabled crime' became 'technology-enabled crime' in later years, see e.g. Kim-Kwang Raymond Choo, Russell G. Smith, and Rob McCusker, *Future Directions in Technology-enabled Crime: 2007-09*, Canberra, Australia: Australian Institute of Criminology, 2007.

[20] See e.g. F. Gregory Lastowka and Dan Hunter, 'Virtual Crimes', *New York Law School Law Review*, vol. 49 (2004): 293-316.

[21] See e.g. Robert W. Taylor, Eric J. Fritsch, and John Liederbach, *Digital Crime and Digital Terrorism* (3rd edition), New York: Prentice Hall Press, 2014.

[22] See e.g. The Council of Europe, Convention on Cybercrime, European Treaty Series No. 185, available at http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm. Last visited June 2015.

[23] See e.g. Chris Westland, 'A Rational Choice Model of Computer and Network Crime', *International Journal of Electronic Commerce*, vol. 1 2(1996): 109-126.

[24] See e.g. Donn B. Parker, *Fighting Computer Crime*, New York: Charles Scribner's Sons, 1983. See also Marc D. Goodman, 'Why the People Don't Care about Computer Crime?' *Harvard Journal of Law and Technology*, vol. 10 3(1997): 465-494, pp. 468-469.

[25] See e.g. United Nations Office on Drugs and Crime, 'Computer-Related Crime', *The 11th United Nations Congress on Crime Prevention and Criminal Justice*, 18-25 April 2005, Bangkok, Thailand, available at http://www.unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf. Last visited November 2015.

technologies in the commission of the offence' of 'computer-related crime' points.[26] Comparing these three terms, it can be noted that 'computer crime' and 'computer related crime' are similar, and that both of them refer to crimes in which the computer plays three different roles, with 'crime by computer' as a subset.

Gradually, terms relating to information technology have appeared to emphasise the technological nature of the crimes discussed in this research. 'High-technology crime' refers to activities that manipulate the computer, cellular phone, or other digital communication device to assist in the performance of criminal activity.[27] 'Technologically enabled crime' or 'technology-enabled crime' refers to 'the type of offending that is most directly related to misuse of [information and communication technology]', including computer facilitated fraud, unauthorised access, malware, intellectual property infringement, industrial espionage, child exploitation and offensive content, exploitation of younger people, transnational organised crime and terrorism, and threats to national information infrastructure.[28] 'Virtual crime', in its narrower sense, equates to 'cybercrime', and refers to 'crimes committed against a computer or by means of a computer'.[29] Its broader meaning refers to all crimes involving technology, particularly the technology of the Internet.[30]

Analysis and comparison of the above terms, and of other terms in use, show that each of these terms has its own context, and therefore has deficiencies in other contexts. The terms focusing on the computer seem to be too independent of network, and the Internet in particular; they refer to crimes in which computers are the target, the tool, or an incidental element. Terms such as 'cybercrime', 'network crime' or 'virtual crime' may refer too much to the network and overlook the involvement of computers. When it comes to other terms such as 'high-technology crime' and 'technologically enabled crime', they are so broad that they encompass crimes relating to other technologies, such as bioengineering technology.[31]

---

[26] See e.g. Richard C. Hollinger, 'Crime by Computer: Correlates of Software Piracy and Unauthorised Account Access', *Security Journal,* vol. 4 1(1993): 2-12.

[27] Larry E. Coutorie, 'The Future of High-Technology Crime: A Parallel Delphi Study', *Journal of Criminal Justice*, vol. 23 1(1995): 13-27, p. 13.

[28] Kim-Kwang Raymond Choo, Russell G. Smith, and Rob McCusker, *Future Directions in Technology-enabled Crime: 2007-09*, Canberra, Australia: Australian Institute of Criminology, 2007.

[29] F. Gregory Lastowka and Dan Hunter, 'Virtual Crimes', *New York Law School Law Review*, vol. 49 (2004): 293-316, p. 296.

[30] *Ibid*.

[31] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 9.

Therefore, since no single term has become generally accepted, this research has adopted 'computer crime' and 'cybercrime' (or 'computer misuse' or 'cyber wrongdoing' if the activities in question may not be criminal) to describe its subject matter. Admittedly, this research could justifiably adopt any of the previously mentioned terms. The reasons for adopting the two terms selected are as follows. At the national level, China, the US, England, and Singapore chose the term 'computer' to describe the nature of the crimes discussed in this research when drafting their legal instruments, such as the US Computer Fraud and Abuse Act 1984 and the English Computer Misuse Act 1990. Following these legislations, scholars also adopted 'computer crime' when discussing relevant laws and phenomena. As the network, especially the Internet, began to play an increasingly significant role in the conducting of criminal activity, computer crime transformed into a cyber-version. In this context, the term 'cybercrime' was developed to emphasise the role of the network in computer crime, and the Convention on Cybercrime is an example of such terminology. Because of its adoption by the Convention, the term 'cybercrime' has become a mainstream way of describing computer crime. The activities described under the Convention encompass roughly the same activities that had already been proscribed by national computer crime laws. At the same time, 'computer crime' is still used, because scholars have become accustomed to using the term 'computer crime', and nations find it less meaningful to replace 'computer crime' (or 'computer misuse') with 'cybercrime' in their domestic legislation. Thus, the term 'cybercrime' can be deemed to be an updated term for 'computer crime', and is gradually becoming more widely accepted; meanwhile, the term 'computer crime' is also frequently used in a habitual manner.

1.2.1.2 Computer crime and computer-related crime

The interrelationship between computer crime and computer-related crime raises problems of definition. As observed above, 'computer crime' and 'computer-related crime' sometimes appear to be interchangeable.

This observation was confirmed when Professor Ulrich Sieber used 'computer crime' and 'computer-related crime' interchangeably in his report,[32] and this interchangeable relationship is also reflected in the research conducted by the experts assigned by the Council of Europe (hereafter the CoE) in the 1980s. These experts stated in their report that '…the

[32] Ulrich Sieber, Legal Aspects of Computer-related Crime in the Information Society: COMCRIME-Study, *prepared for the European Commission*, 1 January 1998, pp. 19-21.

committee, throughout this study, uses the term "computer-related crime" or "computer crime"'.[33]

After years' of analysis and discussion, 'computer-related crime' has become a separate concept, and is generally used to refer to crimes facilitated by computers in more recent research. For instance, the US Department of Justice uses 'computer-related crime' to refer to conventional crimes in which the computer is used as a tool.[34] Similarly, in the 1990s, experts for the CoE defined computer-related crime as 'ordinary crimes that are frequently committed through the use of a computer'.[35] It can thus be seen that in these research, computer-related crime is actually a subset of computer crime, and is used to refer to crimes in which a computer is used as the tool.

1.2.1.3 Cybercrime and economic crime

The interrelationship between cybercrime and economic crime can also cause problems. Some scholars have suggested that, for the most part, cybercrime belongs to the area of economic crime, and is thus nothing more than ordinary economic crime.[36] Indeed, from the perspective of economic crime, some criminals do use computers and the Internet to conduct their crime. However, from the perspective of cybercrime, committing a crime for material gain is only a subset of cybercrime. Admittedly, a significant amount of cybercrime is carried out with the intention of material gain,[37] but cybercrime is not always conducted for that. Taking the dissemination of offensive content as an example: it can be both economically motivated, such as the distribution of child pornography for a fee, and non-economically motivated, such as posting racist comments online. In some jurisdictions, such as the United States, the distribution of offensive content is regarded as a crime only when it is conducted on a 'business scale', meaning that the offender must have done it with the intention of making a profit on a large scale. In other jurisdictions, like Singapore, the distribution itself is

[33] The Council of Europe, Recommendation No. R (89) 9 on Computer-related Crime and Final Report of the European Committee on Crime Problems, *Strasbourg 1990*, p. 13, available at http://www.oas.org/juridico/english/89-9andfinal%20Report.pdf. Last visited May 2015.

[34] See e.g. Computer Crime and Intellectual Property Section, US Department of Justice, *The National Information Infrastructure Protection Act of 1996*, Legislative Analysis, 1996.

[35] Article 79 of the Explanatory Report of the Convention on Cybercrime.

[36] The Council of Europe, Recommendation No. R (89) 9. See also Stein Schjølberg and Amanda M. Hubbard, 'Harmonizing National Legal Approaches on Cybercrime', *Geneva: International Telecommunication Union (Document: CYB/04*), 10 June 2005.

[37] Russell G. Smith, Peter Grabosky, and Gregor Urbas, *Cyber Criminals on Trial,* Cambridge: Cambridge University Press, 2004, pp. 9-10.

seen as a sufficient ground to pursue criminal liability. It can thus be assumed that, under certain circumstances, 'cybercrime' overlaps with 'economic crime'.

1.2.1.4 Cybercrime and intellectual property infringement

The concepts of cybercrime and intellectual property infringements may also overlap under certain circumstances. From the perspective of intellectual property infringement, most infringements of intellectual property initially incur civil remedies and only a small proportion lead to criminal sanctions, depending on the scale and consequences of the infringement. However, as a result of the growing availability of intellectual products in digital format, intellectual property infringement can now be conducted on a scale which was previously not possible, and can potentially cause more severe damage.[38] The necessity for a response in the criminal law to deal with such cases has gradually been recognised, particularly since the appearance of video–cassettes, file-sharing and cloud storage.[39] The responses in the criminal law field fall mainly into two categories: using existing criminal sanctions, and introducing additional criminal provisions.[40] From the perspective of cybercrime, intellectual property offences committed using a computer represents only a small subset. Strictly speaking, they are in fact a subgroup of 'computer-related crime', since it is actually conventional crime in which the computer is used as a tool.

1.2.2 Classification of cybercrime

The ways of classifying cybercrime vary in a similar way to the terms describing cybercrime. The US Department of Justice divides computer crime into three categories:

> '(1) crimes in which the computer or computer network is the target of criminal activity, such as hacking and impairment of a computer system;
>
> (2) traditional offences where the computer is a tool used to commit the crime, such as child pornography and online fraud; and

[38] See e.g. Breana C. Smith, Don Ly and Mary Schmiedel, 'Intelectual Property Crimes', *American Criminal Law Review*, vol. 43 (2006): 663-713.

[39] Jonathan Clough, *The Principles of Cybercrime,* Cambridge: Cambridge University Press, 2010, p. 223.

[40] See David S. Wall and Majid Yar, 'Intellectual Property Crime and the Internet: Cyber-Piracy and "Stealing" Information Intangibles', in Yvonne Jewkes and Majid Yar (eds.), *Handbook of Internet Crime* (2nd edition), Oxford: Routledge, 2011, pp. 265-266.

(3) crimes in which the use of the computer is an incidental aspect of the commission of the crime but may afford evidence of the crime, such as addresses found in the computer of a murder suspect.'[41]

Australian scholars adopt a similar three-group classification:

'(1) crime that involves the use of digital technologies in the commission of the offence, such as online fraud and dissemination of offensive materials electronically;

(2) crime that is directed at computing and communication technologies themselves, including unauthorised access to computers and computer networks, and crimes involving vandalism and invasion of personal space like cyber stalking; and

(3) crime that information technology is incidental to the commission of other crimes.'[42]

Comparing these two methods of classification, it can be observed that the difference between them involves vandalism and the invasion of personal space. Under the US classification, vandalism and the invasion of personal space belong to conventional offences where the computer is used as a tool, while in the Australian classification, they fall into a group containing hacking and the impairment of computer systems. The third categories in both classifications are roughly the same, concerning crimes in which a computer is merely used incidentally.

Other methods of classification include categorising cybercrimes into: internet fraud (credit card fraud), computer hacking/network intrusion (hacking for political reasons and spam), cyber piracy (software piracy), the spreading of malicious code (spreading of computer viruses) and others (identity theft, child pornography);[43] or: computer fraud, computer forgery, damage to computer data and programs, unauthorised infringement of a protected

[41] Computer Crime and Intellectual Property Section, US Department of Justice, *The National Information Infrastructure Protection Act of 1996*, Legislative Analysis, 1996.

[42] Russell G. Smith, Peter Grabosky, and Gregor Urbas, *Cyber Criminals on Trial,* Cambridge: Cambridge University Press, 2004, p. 7.

[43] Weiping Chang, Wingyan Chung, Hsinchun Chen and Shichieh Chou, 'An International Perspective on Fighting Cybercrime', *Intelligence and Security Informatics Lecture Notes in Computer Science*, vol. 26 (2003): 379-384.

computer program and unauthorised access to, and interception of a computer system;[44] among others.

This research adopts the US classification, but it uses the classification from a different perspective – that of legal interests – to address the issue of whether cybercrime is an entirely new category of offence shairing no similarity with its offline counterparts, or is merely conventional crime committed in new ways. Using this perspective, this research classifies the first category of cybercrimes as the '**genuine cybercrime**', emphasising that the interests threatened by them are entirely new, and include the security of computers and the security of data. The second category is the '**traditional crimes facilitated by computers**', referring to crimes that already exist in the criminal law, but for which new opportunities have been opened up by computers and the network. The interests threatened by this category are already protected under existing criminal laws. The third category normally refers to situations where a computer is used to prepare for an offence, such as searching for the home address of the target. In these third scenarios, the activities are not normally regarded as a complete offence, but rather as the inchoate offence. This thesis focuses on the first two categories, with some limited discussion of crimes which fall into the third category when national cybercrime legislation entails relevant activities.

1.3 Problem Statement: the scale of cyber wrongdoing and the challenges it poses to criminal law

> 'The outdated laws and the rapid development of information and communication technology precisely constitute a contradiction; endless network issues, therefore, can rarely be solved relying on the traditional legal principles and provisions.'[45]

1.3.1 The scale of cyber wrongdoing

The various forms and diverse purposes of cyber wrongdoing complicate the formulation of measures to tackle it. Initial concerns about unauthorised access to private information soon expanded into concerns that computers could be used to facilitate further crimes. Threats to property were joined by threats to the security of information, and even to the security of nation. Worsestill, these threats have increased at an alarming scale. Taking China as an

[44] Organization for Economic Co-operation and Development, OECD, *Computer-Related Criminality: Analysis of Legal Policy*, Organization for Economic Co-operation and Development, 1986.

[45] Wang Sujuan and Li Kunkun, '"恶意软件"的法律性质及法律调整 (The Legal Nature and Legal Adjustment of Malwares), *Tequ Jingji* (Special Zone Economy), 5(2011): 264-266, p. 265.

example. Statistics show that hacking, malware, phishing websites and emails, and spam or fraudulent message and phone calls are the four main forms of activities which threaten the security of computers and data in China.[46]

Hacking

Hacking became a social problem in China after the mid-1990s,[47] and is often conducted for financial gain, for revenge, or for advance political motivations.[48] People who perform hackings are known as hackers. After discovering the vulnerabilities of computer systems, hackers may exploit them to impair the systems, delete data, or even manipulate public services controlled by the hacked computers. Hackers are no longer limited to the ranks of well-trained experts. On the contrary, nowadays hackers can be hired, and hacking tools can be purchased. Such easy access to hackers and hacking tools exacerbates the already rampant problem of cyber wrongdoing. Moreover, the idea that it could be exploited by terrorists – the potential risk of so-called cyber-terrorism – is of great concern to many States.

Malware

Malware is malicious code (or software) which seeks to 'disrupt, damage or steal information from computer systems'.[49] It includes viruses, worms, Trojan horses and others.[50] It is often attached to popular websites and communication tools in order to spread. For example, if attached to files or websites, malware downloads into computers, smart phones or other network terminals when the file is opened or the website is visited.[51] Once inside the system of the computer, it works by deleting files, impairing systems and functions, stealing information and passwords, and visiting malicious websites. Malware can also exploit existing vulnerabilities of systems, making its entry and manipulation of the system difficult to detect so as to remain unnoticed.

Phishing websites and emails

---

[46] CNNIC, 'The Statistical Report on Information Security of Chinese Netizens 2013', available at http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/mtbg/201312/P020131219359905417826.pdf. Last visited November 2015.

[47] Lennon Yao-Chung Chang, *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait*, Cheltenham, UK·Northampton, MA, USA: Edward Elgar Publishing, 2012, p. 32.

[48] *Ibid.*

[49] Lennon Yao-Chung Chang, *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait*, Cheltenham, UK· Northampton, MA, USA: Edward Elgar Publishing, 2012, p. 24.

[50] *Ibid.*

[51] See the item 'Malware', available at http://us.norton.com/security_response/malware.jsp. Last visited November 2015.

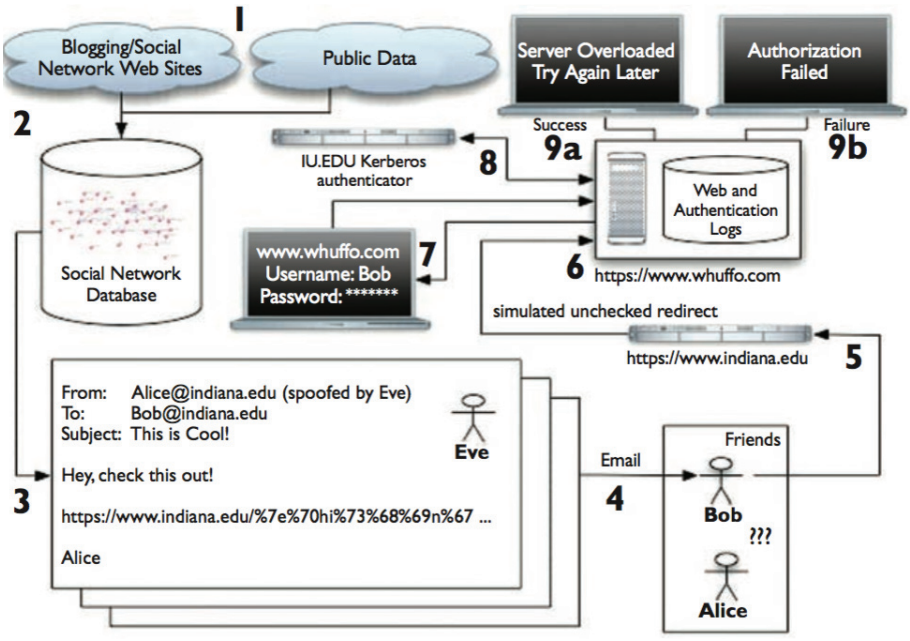
Phishing is the name given to an attack which attempts to acquire sensitive information fraudulently from a victim by impersonating a trustworthy entity.[52] Phishers use social engineering or emails to direct the user to a website where the user is persuaded to divulge personal information, such as account details and passwords or credit card information; the website then captures and steals this information.[53]

Generalised by Tom Jagatic, Figure 1.4 illustrates a typical phishing scheme.

[52] Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer, 'Social Phishing', *Communications of the Association for Computing Machinery*, vol. 50 10(2007): 94-100, p. 94.

[53] For more details see the item 'Phishing', available at http://www.webopedia.com/TERM/P/phishing.html. Last visited November 2015.

Figure 1.4 Proceeding of a phishing scheme



(Source: Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer, 'Social Phishing', Communications of the Association for Computing Machinery, vol.50 10(2007): 94-100)

In stage 1, Eve (the phisher) collects data from blogging, social networks and other public databases. Then, by correlating the data collated in this way, she establishes a database, as shown in stage 2. Eve, pretending to be 'Alice' – Bob's friend – sends Bob a message containing a hyperlink directing him to a phishing website, as stages 3 and 4 demonstrate. Bob clicks on the hyperlink contained in the message, intending to connect to Indiana.edu, but he is, in fact, redirected unnoticed to whuffo.com – a phishing website (stages 5 and 6). In stage 7, Bob is prompted to enter his University credentials, such as his username and password. In stage 8, Bob's credentials are checked. If his credentials are verified, Bob has been successfully phished, as stage 9a shows; if not, the 'phishing expedition' has not been successful on this occasion (stage 9b).

Spam or fraudulent message and phone calls

The perpetrator of this type of wrongdoing distributes junk advertisements or fraudulent information by sending messages or making phone calls. Typical forms include informing the

user they have won a prize, pretending to be a friend trying to borrow money, and making phone calls and hanging up before the victim answers in order to profit from premium rate charges if the victim calls back.[54]

The complexity of the forms taken is one aspect of the scale of cyber wrongdoings. The significant number of reported cyber incidents is the other aspect, as the following figures show.

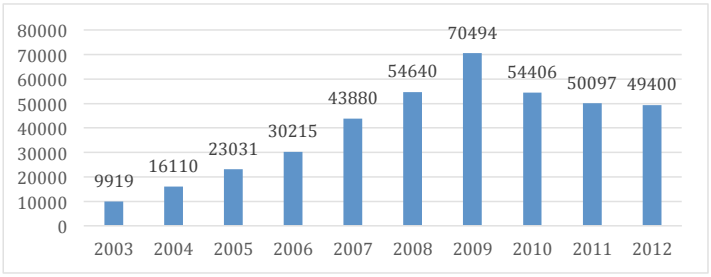
Figure 1.5 Numbers of incidents of malicious cyber activities affecting/reported by individual netizens in China

	Valid report	Start investigation	Inform the reporter to file the case to local police
2013	43828	2813	
2014	87229	6295	5095
2015	110320	2663	14724

(Source: 网络违法犯罪举报网站 (Internet Crime Reporting Centre), data is collected and calculated on the basis of monthly and annual reports)

[54] CNNIC, 'The Statistical Report on Information Security of Chinese Netizens 2013', available at http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/mtbg/201312/P020131219359905417826.pdf. Last visited November 2015.

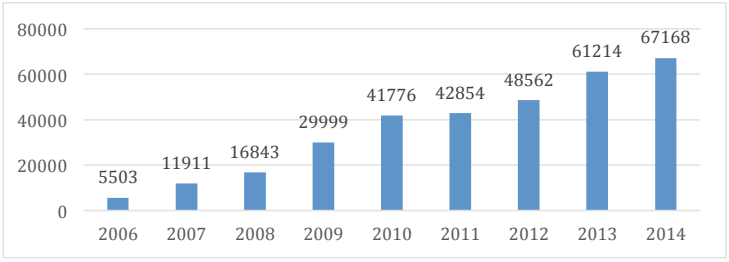
Figure 1.6 Numbers of reported incidents of malicious cyber activity targeting US Department of Defence's system from 2003-2011, with projection for 2012[55]



(Source: US-China Economic and Security Review Commission, USCC 2012 Annual Report, November 2012.

**Data of 2012 is estimated since when making this Figure numbers of reported incidents of malicious cyber activity was not available.)*

Figure 1.7 Information security incidents affecting systems supporting the federal government reported to the U.S. Computer Emergency Readiness Team by federal agencies, fiscal years 2006 through 2014



(Source: US Government Accountability Office analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014, April 2015. | GAO15-573T)

[55] Data shown in Figure 1.6 only includes incidents that source material linked to China. This points at the malicious cyber activities that highly possibly originated from China and targeting the US Department of Defence's system. The drop from 2010 indicates the political intervene of the Chinese and American governments. For instance, Google decided to retreat from China in 2010. The '2012 Annual Report of the US-China Economic and Security Review Commission' is available at http://www.uscc.gov/Annual_Reports/2012-annual-report-congress. Last visited January 2016. For detailed information on Google retreated from China, see e.g. 'China's Internet Crackdown Forced Google Retreat', *The Guardian*, 13 January 2010, available at http://www.theguardian.com/technology/2010/jan/13/google-retreat-china-crackdown-censorship. Last visited February 2016. See also '谷歌为何退出中国' (Why Does Google Retreat from China), *FT 中文网* (FT Chinese), 25 March 2010, available at http://www.ftchinese.com/story/001031904?full=y. Last visited February 2016.

The various forms of cyber wrongdoing and the above figures demonstrate the criminal opportunities which have arisen because of information and communication technology. These present a huge potential risk to the society.

1.3.2 The challenges to criminal law

Legal regimes are developing various strategies aimed at reducing the risk posed by cyber wrongdoing, and legislation is an indispensable part of their strategy. However, research has identified the limited effectiveness of legislations in tackling cyber wrongdoing, especially when it comes to combating cybercrime.[56] At the national level, the limited coverage of traditional criminal provisions, the transitional nature of cybercrime, and the conflicts arising from jurisdictional issues are the main problems. At the international level, the inconsistencies among national legislations make the situation even worse.

The first problem faced by criminal law systems is that existing criminal offences fail to cover the newly emerged forms of cyber wrongdoing. The most frequently cited case – the 'Love Bug' virus case – illustrates this problem. In 2000, the Love-Bug virus appeared in Hong Kong and had raced around the world within two hours.[57] By destroying files and stealing passwords, it impaired millions of computers, including computers used by the US National Aeronautics and Space Administration (hereafter NASA) and the UK Parliament.[58] The losses caused by this virus have been estimated to be in the region of $10 billion, with victims in as many as 20 countries.[59] Experts traced the virus to the Philippines, and police officers from the Philippines National Bureau of Investigation immediately started an investigation. However, the police were unable to obtain a warrant to search for evidence, because the Philippines had no cybercrime legislation and so there was no offence as creating

---

[56] See e.g. Neal Kumar Katyal, 'Digital Architecture as Crime Control', *The Yale Law Journal,* 8(2003): 2261-2289.

[57] See e.g. Lev Grossman, 'Attack of the Love Bug: It Came. It Flattered. It Wreaked Havoc on the Internet. Why Are We so Vulnerable? What Can Be Done?' *Time*, 15 May 2000, available at http://edition.cnn.com/ASIANOW/time/magazine/2000/0515/cover1.html. Last visited January 2015.

[58] See e.g. Lee Davidson, 'Love Bug Report Shows Where U.S. is most Vulnerable: NASA, Social Security and VA among Weak Spots', *Deseret News*, 19 May 2000, available at http://www.deseretnews.com/article/760852/Love-bug-report-shows-where-US-is-most-vulnerable.html?pg=all. Last visited January 2015.

[59] See e.g. Mike Ingram, '"Love-Bug" Virus Damage at $10 billion', *World Socialist Web Site*, 10 May 2000, available at http://www.wsws.org/en/articles/2000/05/bug-m10.html. Last visited January 2015.

and disseminating a computer virus.[60] Given this context, the police tried to apply for a warrant under existing offences – theft and credit card fraud to be precise – and did finally obtain one. The suspect was subsequently identified and arrested. However, the prosecutors encountered the same problem: under which offence should the suspect be prosecuted. The prosecutors also charged the suspect with theft and credit card fraud. The Department of Justice in the Philippines ultimately ruled that the credit card fraud provisions could not be applied to computer hacking, and there was insufficient evidence to support the charge of theft,[61] so the suspect escaped punishment, despite the fact that he had caused a massive amount of damage in 20 countries.

Other countries have also attempted to apply existing criminal provisions to cyber wrongdoing in similar situations; the UK and the US are two examples. However, despite years of attempting to do so, neither of these has ever succeeded in applying the existing provisions to prosecute cyber wrongdoing. What they did do, however, was confirm that the existing provisions had been drafted without foresight of the future emergence of computers and the development in information technology, rendering existing criminal provisions either inapplicable or inappropriate.[62] Cyber-specific legislation was eventually enacted in both these countries.

The second problem is that even where there are cyber-specific offences on the statute books, the transitional nature of cybercrime can blur their scope. 'The criminal sanction is the most drastic of the State's institutional tools for regulating the conduct of individuals,' thus the scope of criminal law must intentionally be limited.[63] However, criminal provisions with such 'intentionally' limited scope soon become outdated when faced with the rapid evolution of cybercrime. Developments in computers themselves can serve as an example. In the field of cybercrime legislation, the concept of the computer undeniably enjoys a central position;

---

[60] See e.g. '"Love Bug" Suspect Detained', *BBC News*, 8 May 2000, available at http://news.bbc.co.uk/2/hi/science/nature/740558.stm. Last visited January 2015.

[61] See e.g. 'Charges Dropped in "Love-Bug" Case', *ABC News*, 21 August 2000, available at http://abcnews.go.com/Technology/story?id=119536. Last visited January 2015.

[62] See e.g. Andrew Charlesworth, 'Legislating against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990', *Journal of Law and Information Science,* 1(1993): 80-93. See also Joseph M. Olivenbaum, '<Ctrl> <Alt> <Del>: Rethinking Federal Computer Crime Legislation', *Seton Hall Law Review* 27(1997): 574-641.

[63] See e.g. Andrew P. Simester and Andreas von Hirsch, *Crimes, Harms, and Wrongs on the Principles of Criminalisation*, Oxford: Hart Publishing, 2011, pp. 19-31.

but computers have evolved as information technology has developed.[64] Elements such as computing and storage capability, which were once used to define a computer, are now no longer exclusively characteristics of what we would call a computer.[65] The question then arises as to whether smart phones, tablets, smart TVs or other devices that are equipped with computing and storage capacities are computers. One case occurred in China demonstrates this conundrum.

In 2010, a Chinese engineer programmed a malware running on smart phones. This malware could manipulate the infected phones to send out messages and register for fee-based telecommunications services. Most of the victims did not initially notice this malware and its money-consuming activities. Within three months, the engineer had 'earned' more than one million RMB from thousands of victims by means of this mobile-phone malware. The total amount of money involved in this case was estimated to be over two million RMB.[66] What's more, with the assistance of a Telecommunications Service Provider, the engineer had established a database – a blacklist of mobile phone users who had complained to the Telecommunications Service Provider (hereafter the TSP). By referring to this, the engineer avoided targeting the users on the list, thereby escaping notice. As a benifit of this cooperation, the TSP received 30% of the total profits.[67] Once the police had identified the engineer, they encountered a problem: were his actions criminal? Analysis of Chinese Criminal Law revealed that although computers were protected, smart phones were not. It therefore followed that these actions were not criminal. As a result, the engineer escaped prosecution and punishment irrespective of the huge losses he caused the victims.

It could be argued that this Smartphone case demonstrates a primary issue with regard to terminology in cases of cyber abuses, and one might think that the remedy of applying a broader interpretation of 'computer' would be the solution. But the problems presented by transitional cyber wrongdoing are more complicated than that. It is not only the concept of the computer that is involved here, but also the ways in which cyber wrongdoing is carried

[64] Jonathan Clough, *The Principles of Cybercrime,* Cambridge: Cambridge University Press, 2010, p. 52.

[65] Yu Zhigang, '三网融合背景下刑事立法的调整方向' (The Direction of the Criminal Law Legislation in the Context of the Combination of Internet, Telecommunication Network and Television Network), *Faxue Luntan* (Legal Forum), 7(2012): 5-12, pp. 6-7.

[66] '全国首例手机病毒恶意扣费案告破，数十万人受害' (Chinese First Mobile Malware Case was Cracked, and the Victims Were Numbered in the Hundreds of Thousands), available at http://news.xinhuanet.com/legal/2011-05/23/c_121447288.htm. Last visited January 2015.

[67] Zhou Bin, '全国首例首例恶意程序案定性难' (Chinese First Mobile Malware Case Faces Difficulty in Judicial Proceedings), *Fazhi Ribao* (Legal Daily), 27 May 2011.

out, as well as the issue of the objects damaged, which are challenging existing criminal provisions, both existing ones and those specifically introduced to combat cyber crime.

Thirdly, the transnational nature of cybercrime confounds traditional principles of jurisdiction. Not only is there an issue of which country has the authority to prosecute, but also the question of which country has priority to prosecute if more than one country claims jurisdiction.[68] Stories are often reported in newspapers in which an actor from country A commits cybercrime in country B by hacking into a computer located in country C. In such a case, which country has the jurisdiction to prosecute the actor and bring them to trial?

In the case of *United States v. Gorshkov,*[69] two Russian nationals, Vasiliy Gorshkov and Alexey Ivanov, were identified as having hacked into the computers of US businesses. To collect evidence for the prosecution, undercover FBI agents established a fake company called 'Invita' in Washington and asked the two Russian hackers to come for an interview with Invita. During the interview, Gorshkov used an FBI laptop to demonstrate his hacking skills. He also accessed his own computer, which was located in Russia, to download his hacking tools. Gorshkov was arrested following this fake interview, and after the arrest, the FBI agents, using a malware, searched the laptop and seized the keystrokes made by Gorshkov, including the username and password that he had used to access his own computer in Russia. Using this login information, the FBI agents logged on to Gorshkov's computer and obtained the evidence they needed. The whole process of search and seizure was conducted without either a warrant or Gorshkov's consent.[70]

When the case came to trial, the Russian defendants argued that 'the evidence obtained from the Russian computer was a product of a seizure that (a) violated the Fourth Amendment and/or (b) violated Russian Law'.[71] The district court of the US rejected the motion, arguing that '(1) the Fourth Amendment did not apply because it does not encompass extraterritorial searches directed at non-US citizens; and (2) even if it did apply, the agent's action was justified under the exigent circumstances exception to the

[68] See Bert-Jaap Koops and Susan W. Brenner (eds.), *Cybercrime and Jurisdiction,* The Hague: T.M.C. Asser Press, 2006, pp. 1-3.

[69] *United States v. Gorshkov*, 2001 WL 1024026, U.S. Dist. LEXIS 26306, available at http://itlaw.wikia.com/wiki/U.S._v._Gorshkov. Last visited February 2016.

[70] *Ibid.*

[71] Susan W. Brenner and Bert-Jaap Koops, 'Approaches to Cybercrime Jurisdiction', *Journal of High Technology Law,* vol. 4 1(2004): 1-46, p. 22.

Fourth Amendment's warrant requirement'.[72] In response to issue (b), the court expressed that '(1) the agents' actions did not violate Russian law and (2) if they did, [the Russian law] has no basis for suppressing evidence in a U.S. proceeding'.[73] Although the American court ruled that there was no violation of the Russian law, the Russian authorities charged the FBI agents with hacking because of what they had done to collect their evidence, and requested their attendance at a trial in Russia. The US government declined to comply.[74]

In this case, the US claimed jurisdiction on the basis that the hacked computer of a US businesses is US territory; while obviously Russia does not accept such jurisdiction. Furthermore, Russia maintains that the FBI agents can be held liable, since they actually collected the evidence by hacking into Gorshkov's computer, which is – in a logical extension of the US court's own argument – Russian territory. The US does not accept this jurisdiction either. Some US academics disagree with the court's decision, and argue that unless there is an agreement between the target country (i.e. the US above) and the source country (i.e. Russia above) such a search and seizure of evidence are a violation of the principle of territoriality.[75] Others supported the judgement, stating that since a consensus between the target country and the source country is difficult to reach, it is permissible to enforce jurisdiction transnationally.[76]

Fourthly, cybercrime also presents problems at the international level. Namely, cross-border cybercrime manifests the inconsistencies of laws and regulations across state boundaries. Cybercrime is national: making it an offence by nature something which national legislation should govern. However, it also has international consequences: a country's position as regards cyber laws or lack of cyber laws can have a considerable impact on other countries. Taking, the Love-Bug case above as an example, after the charges had been dismissed, the US, a country which did have cyber laws, expressed its intention to extradite the suspect. This

---

[72] *Ibid.*

[73] *Ibid.*

[74] Cassim Fawzia, 'Formulating Specialized Legislation to Address the Growing Specter of Cybercrime: A Comparative Study', *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad,* vol. 12 4(2009): 36-79, p.45.

[75] Seitz Nicolai, 'Transborder Search: A New Perspective in Law Enforcement', *Yale Journal of Law and Technology,* 7 (2004): 23-50.

[76] See e.g. Jack Goldsmith, 'The Internet and the Legitimacy of Remote Cross-Border Searches', *University of Chicago Legal Forum,* vol. 1 (2001): 103-118.

attempt failed, however, because extradition treaties require 'double criminality', and the Philippines had no cyber laws.[77] Put another way, 'the Philippines' failure to implement cybercrime legislation meant that a Philippine national could inflict damage in twenty countries but suffered no consequences for his acts; the failure to have legislation was inadvertent, but it still impacted around the globe.'[78] In this context, to encourage the harmonisation of cybercrime legislation and global cooperation, dozens of regional and international organisations have carried out a series of surveys, reviews and seminars about drafting standards and legal obligations to harmonise domestic laws against cybercrime.[79] These regional and international organisations include the United Nations, the Group of Eight (hereafter the G8), the Organisation for Economic Co-operation and Development (hereafter the OECD), the Council of Europe, and others.

Generally speaking, to solve the problems arising from cybercrime, countries such as China, Canada, the United States and the United Kingdom, as well as organisations such as the Council of Europe, have reviewed their criminal law and issued new cyber-specific legislation or inserted cyber-specific provisions into existing criminal laws. Against such background, a systematic approach towards criminal law to regulate cybercrime has become

[77] See e.g. Seth Mydans, 'Philippine Prosecutors Release "Love Bug" Suspect', The New York Times, 10 May 2000, available at http://partners.nytimes.com/library/tech/00/05/biztech/articles/10virus.html. Last visited January 2015.

[78] Marc D. Goodman and Susan W. Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace', *International Journal of Law and Information Technology*, vol. 10 2(2002): 139-223, p. 142.

[79] For the efforts taken under the framework of the United Nations, resolutions such as Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December on 'Combating the Computer Misuse of Information Technology', Resolutions 57/239 of 20 December 2002 on 'Creation of a Global Culture of Cybersecurity' are passed by the United Nations General Assembly, addressing various ways States can adopt to combat cybercrime.

For the efforts taken by the Group of Eight, in 1997 it adopted *Ten Principles* to ensure that no criminal receives safe haven anywhere in the world. *Ten Principles* are available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%208%20Communique_en.pdf. Last visited January 2015.

For the efforts of the OECD, it appointed an expert committee to discuss computer-related crimes and the need for changes in criminal laws in 1983. This committee submitted an analysis of legal policy on computer-related crimes in 1986. The OECD also established a committee on Information, Communications and Computer Policy (ICCP) to analyse related policy, yet focusing on the Internet economy.

As for the efforts taken by the Council of Europe, this thesis will discuss them in detail later. For more information on regional and international activities, see e.g. Stein Schjølberg and Amanda M. Hubbard, 'Harmonizing National Legal Approaches on Cybercrime', *Geneva: International Telecommunication Union (Document: CYB/04),* 10 June 2005. See also Marc D. Goodman and Susan W. Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace', *International Journal of Law and Information Technology*, vol. 10 2(2002): 139-223.

a significant focus for scholars, such as Donn Parker, Orin S. Kerr, David S. Wall, Susan W. Brenner, Majid Yar and Jonathan Clough.[80]

1.4 Research Question and Research Structure

1.4.1 Research question

The cases described above illustrate the main problems posed by cyber wrongdoing for current criminal law systems. Identifying these problems is instrumental in determining criminal laws and approaches that may contribute to the fight against cybercrime. This thesis, through comparative research, intends to answer the central question: *how can the criminal law be adapted to regulate cybercrime*. This central question contains four aspects, which together contribute to revealing the legislative approaches a jurisdiction may take to adapt their criminal law so as to regulate cybercrime. These four aspects are:

Aspect 1: Do we need a cyber-specific legislation to regulate cybercrime?

Aspect 2: If we do need this specific legislation, what the adequate and systematic approaches can this legislation take to determine and regulate cybercrime?

Aspect 3: What principles are sufficient and appropriate to determine jurisdiction over cybercrime?

Aspect 4: What is the function and influence of the Convention on Cybercrime in shaping appropriate legislation and fostering international cooperation against cybercrime?

To shed light on these four aspects, three sub-questions are discussed in this research:

(1) What are the origin and evolution of cybercrime legislation in the selected legal regimes?

(2) What legislative approaches do the legislators take in the field of the criminal law in relation to cybercrime and the issues they address?

[80] See e.g. Donn B. Parker, *Fighting Computer Crime: A New Framework for Protecting Information*, New York: John Wiley & Sons, 1998. Orin S. kerr, *Computer Crime Law* (3rd edition), Minnesota: West Academic Publishing, 2012. David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge: Polity, 2007. Susan W. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Boston: Northeastern University Press, 2012. Majid Yar, *Cybercrime and Society* (2nd edition), London: SAGE Publication, 2013. Jonathan Clough, *The Principles of Cybercrime* (2nd edition), Cambridge: Cambridge University Press, 2015.

(3) On the basis of previous exploration and analysis, how can the criminal law be adapted to regulate cybercrime?

1.4.2 Research structure

This thesis can be divided into three steps corresponding to the three sub-questions. The first step is to unveil the development of cybercrime legislation in the selected legal regimes through historical review, contributing to a better understanding of the rationales on which cybercrime legislation has been made and amended. The second step is to review the current cybercrime legislation of the selected legal regimes and examine the legislative approaches to combating cybercrime reflected in these legislations. The third step is to analyse and compare the historical evolution and current approaches adopted, so as to reach a better legislative design for regulating cybercrime and answer the central research question of how to adapt the criminal law to regulate cybercrime. Since the first two steps are discussed together when analysing each individual legal regime's approach, the substantial text of this thesis consists of two parts: Chapters 2 – 6 cybercrime legislation in the selected legal regimes, and Chapter 7 comparison, conclusion and recommendation.

Chapter 2 presents an analysis of cybercrime legislation in China. It contains three substantial sections: 2.2 provides an overview of the Chinese system for regulating cyber wrongdoing, including legislation, administrative regulations, and departmental rules. 2.3 and 2.4 provide exploration and analysis of Chinese cybercrime legislation both in the past and in the present.

Chapter 2 is followed by four Chapters with respect to one international convention and three cybercrime legislations at the national level. Namely: Chapter 3, the Convention on Cybercrime of the Council of Europe (CoE); Chapter 4, Cybercrime Legislation in the US; Chapter 5, Cybercrime Legislation in England; and Chapter 6, Cybercrime Legislation in Singapore. Each of these chapters is structured in such a way as to explore the origin and evolution of its legislation against cybercrime, to analyse the current cybercrime legislation, to explore the issues most heatedly discussed in relation to this legislation, and to identify the legislative approaches this legislation has taken to address the problems presented by cybercrime. Based on the framework of the Convention on Cybercrime of the CoE, the framework used to examine offences relating to cyberspace contains two categories:

(1) offences against the security of the computer

(2) traditional crimes facilitated by computer.

Chapter 7 provides observations on the selected legal regimes by comparing statutory provisions and their applications regarding cybercrime. Based on the comparison, the conclusion of this thesis is presented through addressing the four aspects of the central research question. In the end, this thesis offers legal recommendations to China, in particular, on the legislative approaches it can take to adapt criminal law.

1.5 Research Methods

1.5.1 Doctrinal research

In order to examine cybercrime legislation in the selected legal regimes and analyse how they have been applied in judicial practice, doctrinal research is used throughout the thesis. Doctrinal research can be explained in a simple way as 'research which asks what the law is in a particular area'.[81] It is the method most frequently used when a researcher intends to investigate and analyse a body of law, including case law and relevant legislation: i.e. the primary sources; and journal articles or other written commentaries on the jurisprudence and legislations: the secondary sources.[82] In answering the first sub-question of how cybercrime legislations have developed in terms of legislative enactment and judicial reasoning, the jurisprudence and legislation are investigated from a historical perspective. As the research goes deeper, current cybercrime legislations and literatures are examined to answer the second sub-question: the legislative approaches each individual legislation takes to deal with cybercrime. At this stage, the application of the legislation, the issues addressed, and the opinions from both the academia and the legislature can be explored. In the end, materials accumulated from the previous research can contribute to identifying and analysing the similarities and divergences among the approaches taken by the selected legal regimes, which serves to answer the third sub-question: what are the legislative approaches to adapt the criminal law to regulate cybercrime.

It is worth noting that the legislative approach taken by a selected legal regime is sometimes complex, and some special regulations on jurisdiction and enforcement power may also reflect its features. In such cases, relevant criminal procedural issues are also addressed if

[81] Mike McConville and Wing Hong Chui (eds.), *Research Methods for Law*, Edinburgh: Edinburgh University Press, 2007, pp. 18- 19.

[82] Mike McConville and Wing Hong Chui (eds.), *Research Methods for Law*, Edinburgh: Edinburgh University Press, 2007, p. 19.

their discussion can contribute to understanding the unique approach taken by the selected legal regime.

1.5.2 Comparative Study

The criminal approaches to tackling cybercrime vary in different countries, not least because of their different legal and cultural traditions. For a better understanding of cybercrime legislation, and to better contribute to the regulation of cybercrime, this thesis has chosen four jurisdictions for its comparative research – China, the United States, England, and Singapore – based on legal traditions, comparability and language. Meanwhile, as suggested above, cybercrime is not only an issue at the level of national law, but also has international influences. Thus, the value of research into cybercrime and its countermeasures would be limited without a discussion of efforts at the international level. For this reason, the Convention on Cybercrime (hereafter the CoC) is also studied, as the most influential international legal instrument on cybercrime.

1.5.2.1 China

Several Chinese legal scholars have conducted comparative research on cybercrime and cybercrime legislation.[83] However, research conducted and written in English is limited. The author has therefore intentionally included China as one of the research subjects in order to provide English readers with detailed information and an analysis of Chinese cybercrime legislation. In addition, China's problems in attempting to use the criminal law to tackle cybercrime serve as a starting point for this research, which also intends to present legal recommendations to China on combating cybercrime.

1.5.2.2 The Council of Europe

The Council of Europe was one of the first major organisations to take measures against cyber wrongdoing in the field of criminal law, and it has also been the most successful.[84] This is not only because by January 2016 the CoC had 54 signatories, but also because the CoC is the most detailed legal instrument addressing cybercrime issues in the international

---

[83] See e.g. Pi Yong, *网络犯罪比较研究* (Comparative Research on Cybercrime), Beijing: Press House of Chinese People's Public Security University, 2005. See also Zhou Wen, '欧洲委员会控制网络犯罪公约与国际刑法的新发展' (Convention on Cybercrime of the Council of Europe and New Development in International Criminal Law), *Law Review*, 3(2002): 79-87. See also Bin Liang and Hong Lu, 'Internet Development, Censorship, and Cyber Crimes in China', *Journal of Contemporary Criminal Justice*, vol. 26 1(2010): 103-120.

[84] For the efforts taken by other regional and international organisations see footnote 77.

arena. The CoE holds the opinion that the consensus on adopting cybercrime legislation that can be achieved at the international level must be built upon in the future in those areas where less international agreement exists;[85] it therefore produces a 'minimum list' of computer crimes by international consensus. At the same time, it also provides a recommended 'optional list' on which an international consensus was harder to reach.[86] By doing so, the CoC serves as a framework upon which specific provisions on cybercrime can be based at the national level.

It should be noted that the CoC is not used as a model law in this thesis. Rather, since it contains detailed and comprehensive descriptions of and guidelines about cyber offences and has had a significant impact on the law-making of States, it is used both as a comparative sample and as a criterion for evaluating the legislative approaches generalised from the domestic cybercrime legislations.

1.5.2.3 The United States and England

The promulgation of specific cybercrime acts in England and the US is one of the reasons to use them as comparison subjects. The legal systems of England and the US have long been regarded as representatives of the common law system, and case law plays a vital role in both of these jurisdictions. However, in the field of cybercrime, the US enacted its specific criminal act at the federal level, the Computer Fraud and Abuse Act as early as 1984,[87] and England also promulgated the Computer Misuse Act in 1990.[88] Why they choose a statutory instrument rather than relying on case law is one of the issues this thesis intends to explore. Their considerations on promulgating new acts can provide insights that facilitate a better understanding of criminal solutions for cyber wrongdoing.

Secondly, both England and the US are parties to the Convention on Cybercrime. Their implementations and reservations of provisions in the Convention can offer some reference for internationally accepted recommendations.

---

[85] Jonathan Clough, *The Principles of Cybercrime,* Cambridge: Cambridge University Press, 2010, p. 22.

[86] These two lists are discussed in detail in Chapter 3, The Convention on Cybercrime of the Council of Europe.

[87] Computer Fraud and Abuse Act 1984 (Coded as 18 U.S.C. § 1030), the United States. Enacted with the name of *The Counterfeit Access Device and Computer Fraud and Abuse Act*, Pub. L. No. 98-473. Changed to *The Computer Fraud and Abuse Act* in 1986.

[88] Computer Misuse Act 1990 (Chapter 18), England.

1.5.2.4 Singapore

The similarity between the Chinese and Singaporean legal systems is one of the main reasons for choosing Singapore as a comparison subject. Given that the legal traditions of England and the US arguably demonstrate a lack of similarity, and thus of comparability, with that of China,[89] Singapore was selected to forestall this criticism. For one thing, Singapore's cybercrime legislation is to a large extent based on English laws,[90] and several provisions in the Singapore Computer Misuse and Cybersecurity Act[91] are borrowed directly from the English Computer Misuse Act. For another, Singapore shares a similar legal tradition with China. Thus, it may share similar problems and considerations when adapting the criminal law to address cybercrime. In this regard, Singapore's experiences and discussions may be more relevant and useful than those of England and the US, especially when it comes to how to learn from jurisdictions with common law traditions.

In addition, much material on Singaporean cybercrime legislation in English is available for comparison, including the legislation, parliamentary discussion and academic analysis.

[89] For the comparability between the Chinese legal system and the English and the American legal systems, see e.g. Ulrich Drobnig, 'The Comparability of Socialist and Non-Socialist Systems of Law', *Tel Aviv University Studies in Law*, 3(1977): 45-57. See also Rodolfo Sacco, 'Legal Formants: A Dynamic Approach to Comparative Law (Instalment I of II)', *The American Journal of Comparative Law*, vol. 39 (1991): 1-34.

[90] For the legal system in Singapore, see e.g. Andrew Phang, 'The Singapore Legal System – History, System and Practice', *Singapore Law Review*, vol. 21 (2000): 23-61.

[91] Computer Misuse and Cybersecurity Act 1993 (Chapter 50A), Singapore. Its name used to be Computer and Misuse Act, and was changed to the current name in 2013.

Chapter 2 The Cybercrime Legislation in China

2.1 Introduction

This Chapter intends to provide an overview and analysis of the legislative framework on cybercrime and its approach in China. Cyber wrongdoing in China is not regulated under a single act or legislation. Rather, it is tackled by a series of instruments at three levels: (1) the criminal law and the Amendments to the criminal law, (2) administrative regulations and departmental rules, and (3) Judicial Interpretations and case law. Section 2.2 starts with an overview on these three levels of the regulatory system regarding cyber wrongdoing. 2.3 limits its focus to the first level, and presents a historical review of cybercrime legislation, with an aim to explore the amendments made to the cybercrime legislation and the rationales behind them. 2.4 subsequently analyses the current legislation and investigates the core contentious issues addressed regarding cybercrime. 2.5 examines the scope of cybercrime both from the perspective of definition and from the perspective of judicial practice. In the end, the principal features of Chinese legislation on cybercrime and its approach are summarised in 2.6.

2.2 An Overview of the Regulatory System Regarding Cyber Wrongdoing

The Chinese regulating system on cyber wrongdoing is a multi-dimensional and comprehensive mechanism to protect the computers and the data stored on the computer.[92] According to the hierarchy of the issuing body, regulations on cyber wrongdoings can mainly be divided into three levels:

(1) the Criminal Law issued by the National People's Congress (hereafter the NPC), and the Amendments to the Criminal Law and Decisions issued by the Standing Committee of the NPC (hereafter the SCNPC);

(2) administrative regulations issued by the State Council (hereafter the SC) and departmental rules issued by the Ministries; and

[92] Hong Lu, Bin Liang and Melanie Taylor, 'A Comparative Analysis of Cybercrimes and Governmental Law Enforcement in China and the United States', *Asian Criminology,* 5(2010): 123-135, p.127.

(3) the Judicial Interpretations issued by the Supreme People's Court[93] (hereafter the SPC) and the Supreme People's Procuratorate[94] (hereafter the SPP) and case law.

Figure 2.1 Chinese regulatory system regarding cyber wrongdoings

Legislator	Chinese term	English term	Title of law
National People's Congress (NPC)	法律	Law	Criminal Law 1997
Standing Committee of National People's Congress (SCNPC)	刑法修正案	Amendment to the Criminal Law	Amendment (VII) to the Criminal Law of the People's Republic of China 2009 Amendment (IX) to the Criminal Law of the People's Republic of China 2015
	决定	Decision	Decisions on Preserving Computer Network Security 2000[95] (hereafter the Decision 2000) Decisions Regarding the Strengthening of Network Information Protection 2012[96] (hereafter the Decision 2012)
Supreme People's Court (SPC) and Supreme People's Procuratorate (SPP)	司法解释	Judicial Interpretation	Provisions on Citation of Such Normative Legal Documents as Laws and Regulations in the Judgements 2009[97] (hereafter the Interpretation 2009) Interpretations (II) of Several Issues on Application of Law in Handling Criminal Cases about Producing,

[93] The Supreme People's Court is the highest judicial organ of the PRC; its primary duty is to supervise the local people's courts. More precisely, it has the authority to hear all kinds of cases, issue Judicial Interpretations, supervise the trials of local courts, and administer national judicial affairs according to the law. Because of the status and authority of the SPC, its Judicial Interpretation is regarded as law in a broad sense and binding to the courts in China.

[94] The Supreme People's Procuratorate is the highest procuratorial organ of the PRC. Its duties include legal supervision and issuing Judicial Interpretation. The former is to ensure the unity and validity of the implementation of national law; the latter is to apply the law in the administration of Justice. In a broad sense, the Judicial Interpretation issued by the SPP is also regarded as law in a broad sense and binding to the Public Prosecution.

[95] *2000 年全国人大常委会关于维护互联网安全的决定* (National People's Congress Standing Committee Decision concerning Preserving Computer Network Security 2000), available at http://www.npc.gov.cn/wxzl/gongbao/2001-03/05/content_5131101.htm. Last visited February 2016.

[96] *2012 年全国人大常委会关于加强网络信息保护的决定* (Decisions Regarding the Strengthening of Network Information Protection 2012), available at http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm. Last visited February 2016.

[97] *2009 年最高人民法院关于裁判文书引用法律、法规等规范性法律文件的规定* (Provisions of the Supreme People's Court on the Citation of Such Normative Legal Documents as Laws and Regulations in the Judgements), *Fa Shi* [2009] No. 14, available at http://www.lawinfochina.com/display.aspx?lib=lawandid=7818andCGid=. Last visited July 2015.

			Reproducing, Publishing, Selling and Disseminating Pornographic Electronic Information via the Internet, Mobile Communication Terminals and Sound Message Stations 2010[98] (hereafter the Interpretation 2010) Interpretations of Several Issues on the Application of Law in Handling Criminal Cases about Endangering the Security of Computer Information Systems 2011 [99] (hereafter the Interpretation 2011) Interpretations on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks 2012 [100] (hereafter the Interpretation 2012) Interpretations on the Application of Law in the Handling of Defamation Cases through the Use of Information Networks 2013[101] (hereafter the Interpretation 2013)
	两高意见	Judicial Opinion	Opinions on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Internet Gambling 2010**[102]**
State Council (SC)	条例	Regulation	Safety and Protection Regulations for Computer Information Systems 1994[103] (hereafter the Regulation 1994)

[98] *2010 年最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释(二)*(Interpretations (II) of Several Issues on Application of Law in Handling Criminal Cases about Producing, Reproducing, Publishing, Selling and Disseminating Pornographic Electronic Information via the Internet, Mobile Communication Terminals and Sound Message Stations 2010), *Fa Shi* [2010] No. 3, available at http://news.xinhuanet.com/legal/2010-02/03/content_12925546.htm. Last visited February 2016.

[99] *2011 年最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释* (Interpretations of Several Issues on the Application of Law in Handling Criminal Cases about Endangering the Security of Computer Information Systems 2011), *Fa Shi* [2011] No. 19, available at http://www.scio.gov.cn/xwfbh/qyxwfbh/document/1004368/1004368.htm. Last visited February 2016.

[100] *2012 年最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定* (Interpretations on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks 2012), *Fa Shi* [2012] No. 20, available at http://www.chinacourt.org/law/detail/2012/12/id/146033.shtml. Last visited February 2016.

[101] *2013 年最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释* (Interpretations on the Application of Law in the Handling of Defamation Cases through the Use of Information Networks 2013), *Fa Shi* [2013] No. 21, available at http://www.spp.gov.cn/zdgz/201309/t20130910_62417.shtml. Last visited February 2016.

[102] *2010 年最高人民法院、最高人民检察院、公安部关于办理网络赌博犯罪案件适用法律若干问题的意见* (Opinions on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Internet Gambling 2010), *Gong Tong Zi* [2010] No. 40, available at http://www.spp.gov.cn/flfg/gfwj/201208/t20120830_2438.shtml. Last visited February 2016.

[103] *1994年计算机信息系统安全保护条例* (Safety and Protection Regulations for Computer Information Systems 1994), *Decree No. 147 of the State Council*.

			Regulations on Managing Network Information Services 2000[104] Regulations on the Protection of Computer Software 2001[105] (revised in 2011 and 2013) (hereafter the Regulation 2001)
Ministries	办法	Measure	Measures for Security Protection in the Administration of the International Networking of Computer Information Networks 1997[106] (revised in 2011) (hereafter the Measure 1997)
	规定（部门）	Provision/Regulation	Regulations on State Secrets Administration for International Networking of Computer Information Systems 2000[107]

2.2.1 Criminal Law, Amendments to the Criminal Law, and Decisions

Laws regarding crime and sanction can only be issued by the NPC and the SCNPC.[108] Legislations at this level contain two parts: the Criminal Law and its Amendments, and the Decisions. The Criminal Law issued by the NPC and its Amendments issued by the SCNPC serve as the basic legal instruments for dealing with cybercrime because of the hierarchy of their issuing bodies. According to the Constitution and the Legislation Law, the NPC is the supreme organ of State power,[109] and it enacts and amends criminal, civil, and state organic laws and other basic laws.[110] The NPC Plenary normally meets once a year to discuss national affairs. Outside the Plenary meetings, the NPC functions through its Standing Committee, i.e. the SCNPC. The responsibility of the SCNPC is to enact and amend laws other than those which can only be enacted by the NPC, and to partially amend and

[104] *2000年互联网信息服务管理办法* (Regulations on Managing Network Information Services 2000), *Decree No. 292 of the State Council*.

[105] *2001年计算机软件保护条例* (Regulations on the Protection of Computer Software 2001), *Decree No. 339 of the State Council.*

[106] *1997年计算机信息网络国际联网安全保护管理办法（2011年修订）*(Measures for Security Protection in the Administration of the International Networking of Computer Information Networks 1997 (2011revised)), *Decree No. 33 of the Ministry of Public Security.*

[107] *2000年计算机信息系统国际联网保密管理规定* (Regulations on State Secrets Administration for International Networking of Computer Information Systems 2000), *January 2000, State Secrecy Bureau*.

[108] Articles 7 and 8 of the Legislation Law, available at http://www.for68.com/new/201007/he375041435912701021299 7.shtml. Last visited June 2015.

[109] Article 57 of the Constitution, available at http://english.gov.cn/2005-08/05/content_20813.htm. Last visited June 2015.

[110] Article 7 of the Legislation Law.

supplement national laws enacted by the NPC when it is not in session, provided that such amendments or supplements do not contravene the basic principles of the national laws.[111]

Cybercrime under the Criminal Law and its Amendments contains five specific offences and one non-specific article, including illegal access to computers (Art. 285), computer interference (Art. 286), failing to fulfil the obligation of supervising information network (Art. 286A), illegal use of the information network (Art. 287A), assistance of cybercrime (Art. 287B) and the non-specific article ruling traditional crimes facilitated by computers (Art. 287).

With regard to the Decision made by the SCNPC, so far the SCNPC has made two Decisions regarding cyber wrongdoings. They are the *Decision on Preserving Computer Network Security 2000* and the *Decision Regarding the Strengthening of Network Information Protection 2012*. Both of them confirm the necessity of regulating cyber wrongdoings. The *Decisions 2000* emphasises the legal liability of the offender, criminally, administratively or civilly.[112] It states that the following six categories of activities that threatening the security of computer network shall be punished under relevant statutory provisions:

(1) offences undermining the safe operation of a computer network, such as attacking a computer information system or telecommunication network;

(2) offences undermining national security and social stability, such as incitement to subvert the state's political power or overthrow the socialist system;

(3) offences undermining the order of the socialist economic market or social management order through the internet, such as the dissemination of pornographic images;

(4) offences infringing personal property and other legitimate rights of individuals, legal persons and other organisations via the internet, such as insulting another person or fabricating facts to slander another person;

(5) other offences that are not covered in points (1) to (4);

[111] Article 7 of the Legislation Law.

[112] Bin Liang and Hong Lu, 'Internet Development, Censorship, and Cyber Crimes in China', *Journal of Contemporary Criminal Justice,* vol. 26 1(2010): 103-120, p.112.

(6) illegal activities that violate the *Regulations on Administrative Penalties for Public Security*[113] via the Internet and are not deemed serious enough to be punished under criminal law; infringements which violate other laws and administrative regulations via the Internet, and are not deemed serious enough to be punished under criminal law or the *Regulations on Administrative Penalties for Public Security*; and infringements which violate civil laws.[114]

From the above wordings one can see that the *Decision 2000* focuses on the computer and network, but not the data or information. As more and more data stored on computers has been stolen and distributed online,[115] the SCNPC issued *the Decisions 2012*[116] to regulate such a phenomenon. The *Decision 2012* focuses on the data stored on digital devices that delivering a citizen's personal identity or that relating to a citizen's personal privacy, and reaffirms that criminal liability should be pursued in accordance with the criminal law where a crime has been committed.[117]

2.2.2 Administrative regulations and departmental rules

Apart from the laws passed by the NPC and the SCNPC, to regulate activities involving computer and network, in particular to deter activities that are 'supposedly detrimental to the interests of the State or the collectives', the Chinese executive organs have issued a series of regulations, including administrative regulations and departmental rules.[118] The administrative regulations and the departmental rules are excluded from the law in the sense

---

[113] In 2006 the SCNPC enacted the Public Security Administration Punishments Law (治安管理处罚法) to replace the Regulations on Administrative Penalties for Public Security (治安管理处罚条例). Worth mentioning, the new *Public Security Administration Punishments Law* is more or less the same as its predecessor *Regulations on Administrative Penalties for Public Security*. Wrongful acts that violate laws yet are not serious enough to pursue criminal liability shall be punished under this new Law as administrative offences. See Yang Xinjing, '刑法与治安管理处罚法竞合问题研究' (The Contradiction between Criminal Law and Public Security Administration Punishments Law), *Renmin Jiancha* (People's Procuratorate), 5(2007): 26-28.

[114] See more details on *2000 年全国人大常委会关于维护互联网安全的决定* (National People's Congress Standing Committee Decision concerning Preserving Computer Network Security 2000).

[115] '《关于加强网络信息保护的决定》综合解读' (Comprehensive Interpretations on the Decision Regarding Strengthening Network Information Protection), *Kai Feng,* 5 January 2013, available at http://www.kaiwind.com/xwzc/news/201301/t165329.htm. Last visited June 2015.

[116] *2012年全国人大常委会关于加强网络信息保护的决定* (Decisions Regarding the Strengthening of Network Information Protection 2012).

[117] See more details on *2012 年全国人大常委会关于加强网络信息保护的决定* (National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection 2012).

[118] Assafa Endeshaw, 'Internet Regulation in China: The Never-ending Cat and Mouse Game', *Information and Communications Technology Law*, 13(2004): 41-57, p.44.

of the Legislation Law 2015.[119] That means they cannot be used as the ruling basis when judges adjudicate criminal cases.[120] However in judicial practice, they can serve as argumentation in judgements. For example, *the Regulation 1994*[121] defines technical terms such as 'computer' which can be used by judges in court. Moreover, they can be deemed as the antecedent of the criminal response, and thus can to some extent imply the future changes in the criminal law. For instance, section 23 of *the Regulation 1994*[122] states that whoever endangers the security of the computer by inputting computer virus or harmful data to computer systems shall be punished. Afterwards, the activities threatening the security of computers were criminalised when the CL was revised in 1997. Another example is regarding *the Measure 1997* (revised in 2011).[123] Section 5(6) of this Measure of 2011 states that citizens should not use the information network to disseminate 'information that propagates feudalistic superstition, obscenity, pornography, gamble, violence, and that instigates crime'. Subsequently in 2015, the Amendment (IX) to the CL criminalises activities that using the information network to disseminate information that propagates obscenity and instigates crimes.

Since executive organs not only produce a large volume of regulations and rules but also frequently change them, it is unrealistic to describe and analyse all of them. Therefore, the following provides only an outline of Chinese administrative regulations and departmental rules rather than a detailed analysis.

2.2.2.1 Administrative regulations

The State Council, as the highest executive organ, issues administrative regulations. It can 'adopt administrative measures, enact administrative regulations and issue decisions in accordance with the Constitution and the laws'.[124] Since the 1990s the SC has published

[119] Article 7 of the Legislation Law rules that only the NPC and the SCNPC can make laws. Article 65 of the Legislation Law rules that the SC can issue administrative regulations in accordance with the Constitution and laws. Article 80 of the Legislation Law rules that Ministries, Committees and other affiliated institutions of the SC can enact departmental rules.

[120] Article 3 of the Provisions of the Supreme Peopl's Court on the Citation of Such Normative Legal Documents as Laws and Regulations in the Judgements, *Fa Shi* [2009] No. 14.

[121] Section 1 of the Safety and Protection Regulations for Computer Information Systems 1994, *Decree No. 147 of the State Council*.

[122] The Safety and Protection Regulations for Computer Information Systems 1994, *Decree No. 147 of the State Council*.

[123] The Measures for Security Protection in the Administration of the International Networking of Computer Information Networks 1997(2011revised), *Decree No. 33 of the Ministry of Public Security*.

[124] Article 89 of the Constitution.

dozens of regulations to control misuses of computers and network. In general, as suggested by Kam C. Wong, these regulations can be categorised into three groups: (1) network monitoring and control, (2) security of network information system, and (3) protection of intellectual property and facilitation of E-commerce.[125]

(1) Network monitoring and control

Regulations under this category are enacted to regulate the network from the aspects of its content, the responsibility of the Internet service providers, and others. For example, the *Interim Provisions on the Management of International Networking of Computer Information Network (1997 revised)* attaches pre-requisites to companies engaged in internet services business.[126] Article 19 of the *Regulations on the Administration of Business Sites of Internet Access Services 2002* further requires such companies to establish a system by means of which unlawful activities on the network can be detected.[127]

(2) Security of network information system

Regulations under this category are issued to protect the security of computer information systems and to prohibit illegal behaviours from jeopardising such systems. *The Regulation 1994* is one such example. As the first official Regulation on computer security, it requested individual companies to establish their own mechanisms to protect computers from being hacked.[128]

(3) Protection of intellectual property and facilitation of E-commerce

As the Internet and E-commerce became an important stimulus to the Chinese economy, hackers rapidly noticed the potential profits in this field. Relevant misuse of them quickly appeared. In this context, regulations protecting intellectual property and E-commerce have been enacted. For example, the *Regulations 2001 (2011 and 2013 revised)* provides a

[125] Kam C. Wong, *Cyberspace Governance in China*, New York: Nova Science Publishers, 2011.

[126] Article 9 of the Interim Provisions on the Management of International Networking of Computer Information Networks, *Decree No. 195 of the State Council.*

[127] See more details on *2002 年互联网上网服务营业场所管理条例* (Regulations on Administration of Business Premises for Internet Access Services), *Decree No. 363 of the State Council*, at http://www.china.org.cn/business/laws_regulations/2007-06/22/content_1214798.htm. Last visited April 2016.

[128] Article 13 of the Regulations of the People's Republic of China for Safety and Protection Regulations for Computer Information Systems 1994, *Decree No. 147 of the State Council*.

safeguard to the rights of the copyright owner of computer software to address the relationships arising in the dissemination and use of such software.[129]

2.2.2.2 Departmental rules

The Ministries can issue departmental rules in the sectors of which they are in charge in accordance with the Constitution and the legislations, decisions, and regulations issued by the NPC, the SCNPC and the SC.[130] In legislation, the departmental rules are regarded as implementations of the laws or regulations deriving from a higher level in the hierarchy.[131] In practice, they are issued for more occasions where statutory legislation or regulation on a certain issue is absent or where loopholes exist.[132] In general, the departmental rules regulating cyber wrongdoings are grouped into four major categories: registration of domain names,[133] network monitoring and control, and security of network information system, and protection of intellectual property and facilitation of E-commerce.[134]

(1) Registration of domain names

Rules under this category perform 'an important mechanism for censorship of Internet website operators: to restrict the creation of new websites and keep track of who the information content providers of a website are'.[135] This series of rules includes the *Measures for the Administration of Internet Domain Names of China 2004*, the *Measures of the China Internet Network Information Centre for Resolving Disputes Regarding Domain Names (2012 Revised)* and others.

---

[129] See more details on the Regulations on the Protection of Computer Software 2001, *Decree No. 339 of the State Council.*

[130] Article 90 of the Constitution; *cf.* Article 80 of the Legislation Law. Several legal scholars regard the power of the Ministries on issuing departmental rules to enhance administrative functions as the most important development in Chinese administrative law since the 1980s. See e.g. Jan Michiel Otto and Yuwen Li, 'An Overview of Law-Making in China', in Jan Michiel Otto, Maurice V. Polak, Jianfu Chen and Yuwen Li (eds.), *Law-Making in the People's Republic of China*, Netherlands: Kluwer Law International, 2000, p. 3.

[131] Article 80 of the Legislation Law.

[132] Jan Michiel Otto and Yuwen Li, 'An Overview of Law-Making in China', in Jan Michiel Otto, Maurice V. Polak, Jianfu Chen and Yuwen Li (eds.), *Law-Making in the People's Republic of China*, Netherlands: Kluwer Law International, 2000, p. 3.

[133] Domain Name System is a distributed, replicated name service whose primary purposes are to map host names into corresponding Internet addresses, map Internet addresses into hostnames, and locate daemons for electronic mail transfer. It gives the world domain suffixes, such as .edu, .com, .gov, and a series of country codes. See e.g. Peter B. Danzig, Katia Obraczka, Anant Kumar, 'An Analysis of Wide-Area Name Server Traffic: A study of the Internet Domain Name System', *ACM SIGCOMM Computer Communication Review*, vol. 22 4(1992): 281-292.

[134] Kam C. Wong, *Cyberspace Governance in China*, New York: Nova Science Publishers, 2011.

[135] *Ibid.*

(2) Network monitoring and control

Administrative rules under this category include the *Provisions on the Interconnection of Designated Networks with Public Networks 1996,* issued by the Ministry of Post and Telecommunications, and the *Implementing Measures for the Provisional Regulations for the Administration of International Networking of Computer Information Networks 1998,* issued by the Information Task Force of the State Council.

(3) Security of network information system

One notable example in this category is *the Measure 1997 (2011 revised).* This Measure states that no individual or unit shall use a network in a way that endangers state security, threatens public interests or infringes a citizen's rights; nor may individuals or units produce or disseminate illegal information.[136]

(4) Protection of intellectual property and facilitation of E-commerce

Rules under this category are enacted to protect intellectual property and promote E-commerce. Two examples are the *Measures for the Registration of Computer Software Copyright 1992*, issued by the Ministry of Machinery and Electronics Industry, and the *Interim Regulations on the Administration of Software Products 1998*, issued by the Ministry of Electronic Industry.

2.2.3 Judicial Interpretation and cases

2.2.3.1 Judicial Interpretation

Judicial Interpretation in China refers to the formal document issued by the SPC and the SPP regarding how to apply certain legislations or provisions in judicial practice, such as in prosecutions and adjudications.[137] Judicial Interpretation can be directly cited in judgements even though they are not law with binding force in the sense of the Legislation Law.[138] The Judicial Interpretations are issued and invoked when the statutory provisions are too general

[136] Article 4 of the Measures for Security Protection in the Administration of the International Networking of Computer Information Networks 1997(2011revised), *Decree No. 33 of the Ministry of Public Security.*

[137] See Article 104 of the Legislation Law of China. See also Chen Chunlong, '中国司法解释的地位与功能' (The Status and Function of China's Judicial Interpretation), *Zhongguo Faxue* (China Legal Science), vol. 111 1(2003): 24-32, p. 25.

[138] Provisions of the Supreme People's Court on the Citation of Such Normative Legal Documents as Laws and Regulations in the Judgements, *Fa Shi* [2009] No. 14. See also Li Wei, 'Judicial Interpretation in China', *Willamette Journal of International Law and Dispute Resolution,* vol. 5 1(1997): 87-112.

to apply or out of date.[139] Therefore, given the rapid development of information technology and the principle that criminal law needs to keep stable and foreseeable, Judicial Interpretations are frequently issued regarding activities in the cyberspace. Specifically, by January 2016 the SPC has issued twenty Judicial Interpretations in relation to cyberspace, among which thirteen are regarding cybercrime, ranging from traditional crimes facilitated by computers and the genuine cybercrimes.[140]

In the field of cybercrime legislation, the Judicial Interpretation mainly functions in two ways: guiding judges on how to apply the existing criminal provisions, and demonstrating the position on cybercrime of the judicial organs. Firstly, in cybercrime cases Judicial Interpretations can guide judges the occasions to which the existing criminal provisions apply, both the traditional criminal provisions and the recently introduced cybercrime provisions. For instance, section 2 of the *Interpretation of the SPC and the SPP on Several Issues Concerning the Specific Application of Law in the Trial of Criminal Cases on Swindling 2011*[141] explicitly rules that sending false information through the Internet shall be punished as fraud. Section 1 of *the Interpretation 2013*[142] rules that anyone fabricating and spreading the facts that damage another person's reputation on the information network shall be punished as defamation. Secondly, since the Judicial Interpretation is frequently issued and updated, it serves to demonstrate the position of Chinese judicial organs on cybercrime,[143] and may imply the future amendments to the criminal law.[144] For example, *the Interpretation 2010* regards the activity of providing Internet connection, network server or online storage service to those who intends to commit cybercrime not as an accessory but as a complete criminal offence.[145] Subsequently in 2015, the legislators affirmed and followed this position

[139] See e.g. Pi Yong, '关于中国网络犯罪刑事立法的研究报告' (Report on China's Criminal Law on Cybercrime), *Xingfa Luncong* (Criminal Law Review), vol. 27 3(2011): 198-257.

[140] Yu Chong, '网络犯罪司法解释的现状考察与未来路径' (On the Status and Future Path of the Judicial Interpretation of Cybercrime), *Xingfa Luncong* (Criminal Law Review), vol. 42 2(2015): 188-211, pp. 189-190.

[141] *2011 年最高院、最高检关于办理诈骗刑事案件具体应用法律若干问题的解释* (Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Specific Application of Law in the Trial of Criminal Cases on Swindling), *Fa Shi* [2011] No. 7.

[142] Interpretations on the Application of Law in the Handling of Defamation Cases through the Use of Information Networks 2013, *Fa Shi* [2013] No. 21.

[143] See e.g. Chen Chunlong, '中国司法解释的地位与功能' (The Status and Function of China's Judicial Interpretation), *Zhongguo Faxue* (China Legal Science), vol. 111 1(2003): 24-32.

[144] Yu Chong, '网络犯罪司法解释的现状考察与未来路径' (On the Status and Future Path of the Judicial Interpretation of Cybercrime), *Xingfa Luncong* (Criminal Law Review), vol. 42 2(2015): 188-211, p. 191.

[145] Section 1 of the Interpretations (II) of Several Issues on Application of Law in Handling Criminal Cases about Producing, Reproducing, Publishing, Selling and Disseminating Pornographic Electronic Information via

of the judicial organs in the Amendment (IX) to the CL by introducing a complete offence as providing assistance to those who intends to commit cybercrime.

According to the substantial issues governed by the Judicial Interpretations in the field of cybercrime, they can be divided into two categories. The first category of Judicial Interpretation includes those directly relating to Articles 285 and 286 of the CL. The most frequently used Judicial Interpretation in this category is *the Interpretation 2011*.[146] This Interpretation provides standards for determining penalties for certain forms of the offences under Articles 285 and 286. For instance, Article 1 of it enumerates several behaviours that should be sentenced to a maximum of three years' imprisonment, such as obtaining ten or more items of personal identifiable information used for payment and settlement, securities trading, futures trading or other online financial services. The second category consists of Judicial Interpretations regarding crimes committed through the use of computers or networks, such as *the Interpretation 2013*[147] on online defamation and *the Interpretation 2010*[148] on producing and disseminating pornographic electronic information.

2.2.3.2 Cases

The SPC is the highest court in Chinese judicial system, and it can 'give interpretations on questions concerning the specific application of laws and decrees in judicial proceeding',[149] and 'supervise the administration of justice by the people's courts at various local levels'.[150] Resulting from this status and the authority, the precedents of the SPC have some influence to future cases. In legislations, China does not have a common law tradition, and thus the precedents are not binding. According to Article 3 of *the Interpretation 2009*,[151] only the laws, legislative interpretations and Judicial Interpretations can be cited as a ruling basis.

---

the Internet, Mobile Communication Terminals and Sound Message Stations 2010, *Fa Shi* [2010] No. 3.

[146] Interpretation of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems, *Fa Shi* [2011] No. 19.

[147] Interpretations on the Application of Law in the Handling of Defamation Cases through the Use of Information Network, *Fa Shi* [2013] No. 21.

[148] Interpretations (II) of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Specific Application of Law in the Handling of Criminal Cases about Producing, Reproducing, Publishing, Selling and Disseminating Pornographic Electronic Information via the Internet, Mobile Communication Terminals and Sound Message Stations, *Fa Shi* [2010] No. 3.

[149] Article 33 of the Organic Law of People's Court.

[150] Article 127 of the Constitution.

[151] Provisions of the Supreme People's Court on the Citation of Such Normative Legal Documents as Laws and Regulations in the Judgements, *Fa Shi* [2009] No. 14.

However, in practice, judgements, especially those made by the SPC, in recent years play an increasingly significant role in judicial proceedings.

Starting from 2010, the SPC has published dozens of *guiding cases* 'to unify the application of the law and safeguard judicial justice nationally',[152] and every court in China is expected to follow these guiding cases when adjudicating similar cases.[153] Among all the guiding cases, one case is in particular relevant to computer crime, which will be analysed in section 2.3 of this Chapter. Additionally, the guiding case system indicates that the SPC intends to and starts to use case law to unify the application of the law nationally. Because of this indication, precedents other than the guiding cases also gain some influence in judicial proceedings.[154] Therefore, the precedents relevant to cybercrime are also addressed in this Chapter.[155]

In sum, Chinese regulating system on cyber wrongdoings is relatively comprehensive and complicated. It is a package of instruments from different legislative levels, with the CL and its Amendments at the centre and the remainder interpretating and supplementing them. In addition, since the criminal law needs to keep stable and foreseeable, the administrative regulations, departmental rules and Judicial Interpretations in fact respond ahead of the CL and its amendments when new problems appear. This system seems to be well integrated, whereas it is commented as 'characterised by multiplicity and overlaps even when they deal with the same terrain'.[156]

2.3 Historical Review of the Cybercrime Legislation in China

The cybercrime legislation in China contains the CL and two Amendments. The CL, when being revised in 1997, included three articles to tackle cybercrime, namely, Articles 285, 286

[152] *2010年最高人民法院印发《关于案例指导工作的规定》通知* (Preamble of Notice of the Supreme People's Court on Issuing the Provisions on Case Guidance 2010), *Fa Fa* [2010] No. 51.

[153] Stephen Tung, 'As Chinese Courts Announce "Guiding Cases", Stanford Law School Helps to Spread the Word', in *Stanford News*, 6 February 2012, available at http://news.stanford.edu/news/2012/february/china-guiding-cases-020612.html. Last visited June 2015.

[154] See e.g. Wang Liming, '我国案例指导制度若干问题研究' (Some Issues on the Guiding Case System), *Faxue* (Law Science), 1(2012): 71-80. In this article the author regards the guiding case system is a system in which precedents are binding to future cases. In this system the precedents are not limited to the guiding cases published by the SPC.

[155] The author has studied all the cases dealt with under Articles 285 and 286 and part of the cases facilitated by computers by December 2015 that recorded in the database PKU Lawinfo. This database is the most frequently used database by scholars when looking for precedents.

[156] Assafa Endeshaw, 'Internet Regulation in China: The Never-ending Cat and Mouse Game', *Information and Communications Technology Law*, 13(2004): 41-57, p.46.

and 287. However, computer crime soon expanded out of the coverage of these three Articles. In response, the Amendment (VII) inserted two sub-sections under Article 285 in 2009 to tackle new forms of cybercrime. Nonetheless, this Amendment showed its limit on deterring cybercrime: the abuse of security holes and other activities continued to spread in cyberspace. Therefore, the Amendment (IX) inserted three new Articles, 286A, 287A and 287B, in 2015. Moreover, it introduces corporate liability for legal persons given that more and more companies started to conduct cyber wrongdoings. In general, the above history can be divided into three periods: the period before the CL was revised in 1997; the period from 1997 to 2008: the first criminal provisions against cybercrime and their application; and the period from 2009 to the present day: amendments and expansions.

2.3.1 Pre 1997: a vacuum in cybercrime legislation

There was no specific criminal provision regarding computer crime before 1997. At that time, judges applied the then existing criminal provisions to computer crime, such as provisions on theft and fraud. For example, in a case happened in 1986, the offender was convicted of theft, even though this case was regarded as the first officially reported computer crime in China.[157]

Case 2.1: Chen Case, Guangdong Province, 1986

> The offender, Chen, was a computer information system operator for a bank. Taking advantage of the opportunities presented by his job, he transferred the bank's money into a designated account of his own by gaining access to the bank's database and changing the data stored on it. He was charged with and convicted of theft.[158]

This case triggered a national discussion on the phenomenon of computer crime, namely, whether crimes with and without the involvement of a computer violated the same provision.[159] This question can be analysed from two aspects. The first one is whether crimes

[157] Kam C. Wong, *Cyberspace Governance in China*, New York: Nova Science Publishers, 2011.

[158] Yu Zhigang, *网络犯罪定性争议与学理分析* (Analysis on the Nature of Network Crimes), Jilin: Jilin Renmin Chubanshe, 2001, p. 1.

[159] Under Chinese criminal law system an offence has four constituent elements: the subject of the offence, the subjective perspective of the offence, the object of the offence, and the objective perspective of the offence. Among them, the subject of the offence refers to the offender; the subjective perspective of the offence means the mental status of the offender when committing the crime (roughly refers to *mens rea*); the objective perspective of the offence refers to the factual grounds of the offence, including the illegal activity, the consequence of the activity and others; and the object of the offence means the legal interests violated by the offender. According to the different objects of different offences, the Chinese criminal law divides offences into different types, and regulates the same type by same or similar criminal provisions.

with computer involved distinguished from the crimes without computer involved. Specifically, if the crimes with computer involved distinguish from crimes without computer involved, traditional criminal provisions do not apply to the crimes with computer involved, and new criminal legislation is thus necessary. Otherwise, traditional criminal provisions apply, and there is no need to draft new legislation. The second aspect is whether there is any substantial difference among various forms of the crimes with computer involved. If there is no substantial difference, the crimes with computer involved constitute one unique type of crime, and one offence is enough for the new legislation. Otherwise, the *mens rea* and the *actus reas* of various forms of computer crime are different, and therefore, more than one offence should be introduced by the new legislation.

With respect to the first aspect, it was suggested that at the very least a new criminal provision regulating the crimes targeting computer is necessary. Chen Lihua, who supported this opinion, argued that criminal law must distinguish between the genuine computer crime and those crimes committed by means of a computer in the first place, and the genuine computer crimes required new criminal provisions.[160] According to him, the genuine computer crimes were those targeting computers, while the crimes committed by means of a computer were those which could be seen as 'traditional' or more conventional crimes, and were facilitated by the use of a computer. To get to this conclusion, he argued that the interest the genuine computer crimes infringed upon were the normal functioning of computers. This interest was newly appeared together with information technology, and not covered by the traditional criminal provisions. Therefore, it was necessary to introduce new criminal offence to deal with those crimes that could destroy or impair computer software and hardware in order to protect the normal functioning of computers.[161] On the contrary, to tackle the crimes facilitated by a computer, for example, fraud and embezzlement, judicial organs could either take advantage of extensive interpretation or make new Judicial Interpretations of the existing criminal provisions, as the judges had done in the case 2.1.[162]

Some other scholars, such as Ma Qiufeng, held an opposite opinion by maintaining that new legislation was not necessary. Also analysing this issue from the perspective of the interest infringed, Ma argued that the interests threatened by crimes involving a computer ranged

[160] See Chen Lihua, '计算机犯罪及立法探讨' (The Discussion on Computer Crime and Its Legislation), *Faxue* (Legal Science), 1(1990): 42-44.

[161] *Ibid.*

[162] *Ibid.*

from state security to property, exactly those areas which were covered by the then existing criminal law. Therefore, all kinds of crimes involving a computer had already been covered by the then existing criminal provisions, and computer-specific provision was thus unnecessary.[163]

With respect to the second aspect of the question, Chen maintained that the genuine computer crimes constituted a unique type of crime as they all threatening the normal functioning of computers.[164] Disagreeing with Chen, Ma argued that under criminal law the computer crime was not a unique type of crime.[165] As Ma explained, although the security of computer threatened by the so-called computer crimes seemed to be a new legal interest arising with information technology, it was not a legal interest under criminal law. In fact, the security of computer encompassed several aspects, such as the security of data and the security of the system of computer. Therefore, the security of computer was not a unique interest, but rather a broad term encompassing several legal interests. Moreover, not all the crimes involving computers violated the security of computer. For example, the crime of theft committed through online banks obviously could not be regarded as violating the security of computer.[166]

Despite the various arguments, the necessity for new and specific criminal legislation was recognised by the legislators, which resulted in the computer-specific provisions when the CL was revised in 1997.

2.3.2 From 1997 to 2009: the criminal provisions against cybercrime and their application

The CL 1997 contains three Articles relating to cybercrime, namely, two computer-specific Articles 285 and 286, and non-computer-specific Article 287. Article 285 outlaws unauthorised access to computers involving state affairs, national defence and sophisticated science and technology.

---

[163] Ma Qiufeng, '中国计算机犯罪概念探析' (The Concept of Computer Crime), in *The Proceedings of the 7th National Computer Security Conference*, Beijing: China Academic Journal Electronic Publishing House, 1992, pp. 177-184.

[164] Chen Lihua, '计算机犯罪及立法探讨' (The Discussion on Computer Crime and Its Legislation), *Faxue* (Legal Science), 1(1990): 42-44.

[165] Ma Qiufeng, '中国计算机犯罪概念探析' (The Concept of Computer Crime), in *The Proceedings of the 7th National Computer Security Conference*, Beijing: China Academic Journal Electronic Publishing House, 1992, pp. 177-184.

[166] Ma Qiufeng, '中国计算机犯罪概念探析' (The Concept of Computer Crime), in *The Proceedings of the 7th National Computer Security Conference*, Beijing: China Academic Journal Electronic Publishing House, 1992.

Article 286 contains three subsections:

(1) the deletion, amendment, addition to or disturbance of the function of a computer information system or causing the failure of a computer information system to work normally;

(2) the deletion, amendment or addition of data or application programs that are stored on, disposed of or transmitted in a computer information system; and

(3) the intentional making or dissemination of a computer virus or any other destructive program that affects the normal operation of a computer information system.

Article 287 states that traditional crimes facilitated by computers, such as fraud, theft, embezzlement, misappropriation, the stealing of state secrets and any other crime committed by means of using a computer.

These three Articles shed light on the two aspects discussed in the last period: (1) whether computer crime is distinguished from traditional crimes, and (2) whether there is any substantial difference among various forms of computer crime. Article 287 indicates the legislative response to the first aspect. It distinguishes between the crimes facilitated by a computer and the crimes targeting a computer. The former is tackled under traditional criminal provisions and the latter is specifically addressed under Articles 285 and 286. With respect to the second aspect, the difference between Articles 285 and 286 reflects that computer crime contains various forms. Article 285 prohibits illegal access to the listed computer information systems so as to protect the data stored on those computers, and Article 286 prohibits the impairment of computer information system and the damage of data. By addressing these two aspects, the CL 1997 demonstrates the legislative approach it takes against cybercrime. Namely, the traditional crimes facilitated by computers are different from the new crimes targeting computers, and for the new crimes, the crimes obtaining access to computers are different from the crimes impairing computers.

However, as network and personal computers had kept on gaining popularity, the coverage of these Articles in the CL 1997 soon became insufficient. Apart from the lack of coverage, the lack of protection for data and the imbalance of the punishments attached to criminal offences also raised problems and triggered discussions.

1) The lack of substantive criminal provisions

Articles 285 and 286 did provide a legal basis for criminalising some computer crimes, but they have one drawback: they did not prohibit illegal access to computers belonging to individuals or companies.[167] For instance, if A hacked into B's computer and obtained data stored on it, provided B's computer continued to function normally (otherwise A violated Article 286), A had not violated the criminal law and would get no punishment. Another example is the so-called 'botnet'.[168] A typical illegal botnet is that a programmer spread a computer malware that can allow the programmer control over the infected computer. This malware successfully infected dozens of computers. By manipulating these infected computers, the programmer can launch cyber-attacks on a large scale. This type of activities does not cause the owners of the infected computers any substantive loss because the infected computers suffered no damage and could continue to work normally. These computers are just 'borrowed' by others and 'returned' after being manipulated. However, it infringes the owner' rights over his computer, especially when 'the owner' includes thousands of people.

The emergence of 'hacker schools' also manifested the lack of coverage of Articles 285 and 286.[169] 'Hacker school' refers to the online educational institutions for people who want to gain knowledge at computer programming. With the Internet, hacker schools had become popular, and provided courses for those intended to learn programming skills. However, some of the schools, teachers, and students abused their knowledge by distributing information about how to gain access to computers illegally or program computer virus; *modus operandi* in other words.[170] In such activities the programmers knowingly imparted the methods for committing computer crime to others, although they did not personally or intentionally commit any crime.

2) The lack of protection for personal information

---

[167] Article 285 of the Criminal Law 1997.

[168] 'Botnet' is a group of 'zombie' computers that infected by a type of malware 'bot'. Botnet allows hackers to take control over the zombie computers at a time and launch cyber-attacks, such as spreading virus, sending spams and committing online theft. See e.g. 'Bots and Botnets—A Growing Threat', *Norton by Symantec*, available at http://us.norton.com/botnet/. Last visited March 2016. See also Ramneek Puri, 'Bots and Botnet: An Overview', *SANS Institute*, 8 August 2003, available at http://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299. Last visited March 2016.

[169] See more details on 中国黑客学校：百万会员，获千万风投 (Chinese Hacker School: One Million Members and 10 Million RMB Venture Investment), *ZOL.COM.CN*, 13 July 2009, available at http://soft.zol.com.cn/140/1407633.html. Last visited February 2013.

[170] Zhao Bingzhi and Yu Zhigang. '计算机犯罪及其立法和理论之回应' (Computer Crime and the Response from Legislation and Legal Theory), *China Legal Science*, 1(2001): 148-163, pp. 149-150.

The mining and distribution of personal information online were rampant during this period, manifesting the lack of protection for personal information in China.[171] The method of mining and distributing personal information mainly consisted of the so-called 'human flesh search' (人肉搜索). 'Human flesh search' refers to the phenomenon happens on the Internet of using online media, such as blogs, to search for and disclose personal information of others – it is in fact a kind of cyber-bullying.[172] It is a mass campaign, aimed at 'searching for the identity of a certain person or the truth about a certain event, whose data collection depends partially on the human resources to filter the information gained from the search engine, and partially on the anonymous or real-name information announcement'.[173]

Such activities may result in a severe violation of the right to privacy. Therefore, some scholars suggested legislating against human flesh search. However, human flesh search to a certain degree reflects the freedom of speech in the online world. To be clearer, if the law forbids human flesh search, the online freedom of speech might be subsequently limited; while if the law allows human flesh search, the right to privacy might be infringed. This issue, i.e. how a fair balance can be struck between these two rights, triggered a national discussion.

Supporters of the idea that criminal law taking human flesh search into its remit opined that such acts had seriously violated the right to privacy, which made the criminalisation reasonable.[174] They maintained that the participants of human flesh search might initially have been seeking truth and justice in their efforts; however, it was precisely justice that they ultimately ignored. A typical human flesh search event is that the participants were alerted to cases via the Internet, and decided that the 'offender' should be 'punished' by private sanctions such as insults and threats. Subsequently, the participants searched for personal information of the 'offender', and then disclose the information online. Netizens who knew

---

[171] Dai Jitao, '从"人肉搜索"看隐私权和言论自由的平衡保护' (Internet Mass Hunting: A Balanced Protection of Privacy and Free Speech), *Faxue* (Legal Research), 11(2008): 40-52.

[172] *Ibid*, p. 40.

[173] Bing Wang, Bonan Hou, Yiping Yao, Laibin Yan, 'Human Flesh Search Model Incorporating Network Expansion and GOSSIP with Feedback', *13th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications*, 2009, available at http://dl.acm.org/citation.cfm?id=1671386. Last visited June 2015.

[174] See e.g. Zhao Xiufang, '试论人肉搜索行为的刑法规制-以刑修七草案为视角' (Argumentation on the Criminal Regulation on Human Flesh Search—From the Aspect of the Draft of the Amendment (VII) to the Criminal Law of PRC), *Fazhi yu Shehui* (Legal System and Society), vol. 34 (2008): 346. See also Shen Yuzhong, '个人信息保护与刑法干预的正当性-兼评刑法修正案七第七条' (The Protection to Personal Information and the Legitimacy of Criminal Intervention-the Comments on Article 7 of Amendment (VII) to Criminal Law), *Journal of Yanshan University (Philosophy and Social Science Edition)*, 6(2009): 84-87.

the 'offender' filtered out the correct information. The information disclosed in this process was not limited to the name, phone number and home address, but also to humiliating experiences and moral defects. With such information, participants could condemn the 'offender' and punish him.[175] The serious harm that could result from such actions were beyond morality, and a response in the field of criminal law was necessary.[176]

Those who opposed the criminalisation of the human flesh search expressed their worry on potential influence on restricting online freedom of speech. They maintained that the freedom of speech is one of the fundamental rights enjoyed by citizens, including that in the online world, and it should not be curtailed.[177] Indeed, the right to privacy needed protection, while such protection should not have a negative effect on the freedom of speech.[178] Apart from the concern over the freedom of speech, the opponents of criminalising human flesh search emphasised the positive aspect of disclosing the truth of a 'case'. They maintained that through doing this, human flesh search could regulate the space beyond the reach of the law and provide people with a new way of obtaining information and justice.[179] Lastly, although it was agreed that in some occasions the human flesh search should be regulated, it was not considered severe enough to be dealt with as a criminal offence.[180] The aim of a human flesh search is to search for truth through the Internet. Admittedly, such activities may infringe other's privacy, but this does not mean that all relevant activities would inevitably lead to infringements of privacy. In occasions where the consequences of human flesh search were

[175] See e.g. Bin Liang and Hong Lu, 'Internet Development, Censorship, and Cyber Crimes in China', *Journal of Contemporary Criminal Justice*, vol. 26 (2010): 103-120.

[176] Zhao Xiufang, '试论人肉搜索行为的刑法规制-以刑修七草案为视角' (Argumentation on the Criminal Regulation on Human Flesh Search—From the Aspect of the Draft of the Amendment (VII) to the Criminal Law of PRC), *Fazhi yu Shehui* (Legal System and Society), vol. 34 (2008): 346.

[177] *Ibid.*

[178] Sun Hongyou, '"人肉搜索"中隐私权的保护' (Privacy Protection in Human Flesh Search), *Internet Law Review*, 2(2012): 232-248. See also Hu Ling, '评人肉搜索"第一案"的三个初审判决' (Three First-Instance Judgements of Human Flesh Search Cases), *Internet Law Review*, 1(2012): 181-193.

[179] See e.g. Lu Fei, '人肉搜索入罪提议引发网民激辩' (The Proposal of Criminalising Human Flesh Search Triggered Heated Debate among the Netizens), *Zhongguo Shuiwu Bao* (China Taxation News), 10 September 2008.

[180] *Ibid*. See also Zhao Xiufang, '试论"人肉搜索"行为的刑法规制—以《中国人民共和国刑法修正案（七）草案》为视角' (Argumentation on the Criminal Regulation on Human Flesh Search—From the Aspect of the Draft of the Amendment (VII) to the Criminal Law of PRC), *Fazhi yu Sehui* (Legal System and Society), 12(2008): 346; Xiong Wenqi, '人肉搜索浅析' (Analysis on Human Flech Search), *Jiangxi Gongan Zhuanke Xuexiao Xuebao* (Journal of Jiangxi Public Security College), 1(2009): 126-128.

severe and the reputation of the 'offender' was damaged, provisions that criminalising insult and slander could apply.[181]

Comparing these two opposite opinions one can notice that their start points are different. For those who supported criminalising human flesh search, it is vulnerable to manipulation and abuse, and thus, adequate supervision and regulation are necessary. For those who opposed criminalisation, freedom of speech is more important than privacy, and thus, the protection of privacy shall not impair the freedom of speech.

3) The imbalance of penalties within criminal law

It was widely admitted that the consequences of cybercrimes could be very severe, not only because of the losses they might cause,[182] but also because the opportunities to further crimes such as online fraud and theft, cybercrime provided.[183] Therefore, there was an increasing demand for punishing cyber criminals. However, one problem arose on how to determine the punishment of cybercrime. Various criteria had been raised, such as the amount of computers damaged, the value of data stolen or deleted, and the total value of money involved, but none of them could solve this problem sufficiently and adequately. Moreover, the consistency between punishments of crime in cyberspace and of crimes in the real world would be hard to maintain. For instance, in Chinese criminal law a sentence is primarily determined by the seriousness of the consequence. According to Article 264 of the CL on theft and Article 1 of *the Interpretation 2013*,[184] the offender shall be sentenced to more than ten years' imprisonment, or even to life imprisonment, if the money stolen exceeds a certain amount ranging from 300,000 to 500,000 RMB.[185] However, as cases have shown, the amounts

---

[181] *Ibid.*

[182] Wu Dahua, '计算机犯罪的原因，趋势及其综合防范' (The Causes, Features and Tendency of Computer Crime and Its Prevention), *Journal of Guizhou Ethic Institute (Philosophy and Social Science),* vol. 72 2(2002): 54-61, pp. 55-57.

[183] See e.g. Qu Cuewu, '因特网上的犯罪及其遏制' (Crimes in Cyberspace and Its Regulation), *Faxue Yanjiu* (Legal Research), 4(2000): 83-100.

[184] *2013 年最高人民法院、最高人民检察院关于办理盗窃刑事案件适用法律若干问题的解释* (Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Theft), *Fa Shi* [2013] No. 8, available at http://www.lawinfochina.com/display.aspx?lib=lawandid=13413andCGid=. Last visited June 2015.

[185] In China, the punishment attached to theft is determined by the amount of money stolen. If the money stolen exceeds a certain amount, the offender will get a heavier punishment. More specific, if the money stolen is above a certain amount, the offender will get more than ten years' imprisonment or even life imprisonment. The local court can determine this amount according to local conditions, as long as it conforms to the SPC's instruction. In this case, the amount of money decided by local court should be within a range from 300,000 to 500,000 RMB.

involved in thefts facilitated by computers and the network could easily reach 500,000 RMB.[186] This meant that those who had committed an online theft might get a remarkably heavy punishment for an offence that was essentially as simple as distributing malware capable of stealing money. Situations like this seem to contradict the principle of proportionality between the offence and the punishment.

2.3.3 After 2009: amendments and expansions

To cover the gaps between law and practice presented by the evolving cybercrime, the SCNPC issued the Amendment (VII) and Amendment (IX) in 2009 and 2015 respectively.

The Amendment (VII) inserts two subsections under Article 285 of the CL, as 285(2) and 285(3), to protect the computers belonging to individuals and companies. Namely, Article 285(2) penalises activities that obtaining the data stored, processed or transmitted in or exercising illegal control over the computer information system that not protected under Article 285(1). Article 285(3) criminalises activities that providing tools that can be used to commit offences under Article 285(1) and (2). The introduction of two new subsections is to respond to the insufficient coverage of computer-specific provisions, as identified in the last period. By doing so, activities that impairing computers belonging to individuals and companies can be tackled under the criminal law.[187]

In addition, to respond to the lack of protection for privacy, the Amendment (VII) inserts Article 253A to protect personal information. However, it does not shed light on human flesh search directly. Article 253A outlaws activities that obtaining personal information illegally and trafficking or providing personal information. It seems that since this Article does not mention how such information is obtained or disseminated, whether the actor obtained the information online does not matter. Therefore, human flesh search falls within the reach of this Article. Disagreeing with this reasoning, Lang Sheng, the then vice-director of the Legislative Affairs Commission (hereafter the LAC) of the NPC, explained that

[186] For example, in a case of online theft happened in 2013, the money involved was over 1,000,000 RMB. See "神马"入侵手机，偷钱百万余元 ("Super House" Invaded Smart Phones and Stole over One Million of RMB), *Jiancha Ribao* (Procuratorial Daily), 17 April 2015, available at http://newspaper.jcrb.com/html/2015-04/17/content_184259.htm. Last visited April 2016.

[187] Yu Zhigang, '网络犯罪与中国刑法应对' (Cyber Crimes and Chinese Criminal Response), *Zhongguo Shehui Kexue* (Social Science in China), 3(2010): 109-126, p. 125.

> 'By containing relevant articles such as Article 253A and 285(2), Amendment (VII) intends to protect personal information and regulate illegal access to a personal computer. When the issue comes to the human flesh search, there are many uncertain factors and it needs more discussion and analysis on the elements constituting a human flesh search under the criminal law.'[188]

Despite the Amendment (VII) does not provide an explicit attitude toward the human flesh search, it follows and enhances the approach of the CL 1997. After this Amendment, the approach of CL regulating cybercrime becomes a 'two points and one dimension' approach: 'two points' refer to Articles 285 and 286, which apply to the genuine computer crimes, and 'one dimension' stands for Article 287, which emphasises the prohibition of traditional crimes which could be committed by taking advantage of the possibilities offered by computers.[189]

The guiding case relating to computer crime published in 2014 also follows this 'two points and one dimension' approach.

Case 2.2: Zang Jinquan Case, Zhejiang Province, 01/06/2011[190]

> Zang Jinquan, the defendant, sent computer software to the victim and enticed him to click the false hyperlink contained in that software. The victim was told that by clicking the hyperlink he would transfer 1 RMB to Zang for online purchase and he clicked. In fact, the link was false and when he clicked the hyperlink, he transferred 305000 RMB to the defendant. The defendant is convicted of theft.

By choosing this case as one of the guiding cases, the SPC indicates that theft or fraud committed through sending false electronic information or hyperlink should be dealt with as theft or fraud.[191] This conviction reflects exactly what Article 287 states, that traditional crimes facilitated by computers should be treated as traditional crimes.

---

[188] '全国人大法工委回应人肉搜索是否入罪问题' (The Response from the LAC of the NPC: Whether to Criminalise Human Flesh Search), *Xinhua News*, 28 February 2009, available at http://news.xinhuanet.com/legal/2009-02/28/content_10917011.htm. Last visited March 2013.

[189] Pi Yong, '我国网络犯罪立法研究-兼论我国刑法修正案七中的网络犯罪立法' (The Study on the Criminal Legislation on Cyber Crimes - the Cybercrime Legislation in Amendment (VII) to the Criminal Law), *Hebei Faxue* (Hebei Law Science), 6(2009): 49-57, p. 50.

[190] *Zang Jinquan Case,* [2011] 浙杭刑初字第91号 (Zhehangxingchuzi [2011] No. 91); *cf.* the Guiding Case No. 27.

[191] The Guiding Case No. 27. In this case the defendant sent computer software to the victim and asked him to

In 2015, the Amendment (IX) introduces three new offences, including situations in which a network service provider has failed to fulfil its management obligations (Art. 286A), those using networks to set up websites to teach people how to commit crime or to provide illegal information (Art. 287A), and those using the network to assist in the commission of cybercrime – whatever crimes targeting or facilitated by computer (Art. 287B). Further, Amendment (IX) attaches criminal liability for those corporations committing crimes under Articles 285, 286, 286A, 287A and 287B.[192]

The promulgation of the Amendment (IX) is to combat the 'black market' behind computer crimes, and penalises relevant activities within this market. Moreover, the Amendment (IX) replaces the previous 'two points and one dimension' approach with a new approach: regarding the information network as a new space to commit crimes.[193] This new space is a parallel world of the offline world, and both of the traditional crimes and the new crimes targeting computers can be conducted in it. Therefore, a new branch of law, or at least a new perspective of interpreting the existing law, is necessary.[194] The amendments made by the Amendment (IX) can be deemed as the first step to establish this new perspevtice.

However, under this new approach, traditional crimes facilitated by computers are not essentially different from the genuine cybercrime. Thus, it blurs the provisions against traditional crime and cybercrime, and further restricts the online freedom. Firstly, any crime can be conducted in this new and parallel space, and therefore it is not necessary to distinguish between the genuine cybercrime and the traditional crimes facilitated by computers. The commission of crimes in the information network becomes the only differentiator for crimes in the online world and the offline world. By doing so, the new approach contradicts the previous approach and confuses the occasions to which traditional criminal provisions apply and to which cybercrime provisions apply. Secondly, under Article 287A introduced in 2015, criminal liability may be pursued only because of the involvement

connect to the false link contained in the software. By doing so the victim was asked to transfer 1 RMB to the defendant's account while in fact he transferred 305000 RMB to the defendant's account. The defendant is convicted of theft.

[192] Corporate liability is not attached to Article 287 because it does not establish any offence, but rather emphasises the application of traditional criminal provisions to traditional crimes facilitated by computer.

[193] See e.g. Yu Zhigang, '网络犯罪的发展轨迹与刑法分则的转型路径' (The Tragectory of Cybercrime and the Future Path of the Criminal Law), *Zhongguo Jianchaguan* (The Chinese Procurators), 4(2014): 44-53. See also Li Huaisheng, '三代网络环境下网络犯罪的时代演变及其立法展望' (The Evolution of Cybercrime in Three Generations of the Information Network and the Law-making), *Faxue Luntan* (Legal Forum), 4(2015): 94-101.

[194] *Ibid.*

of the information network in a certain activity. Moreover, under 287B preparing or assisting a crime regarding the information network is now regarded as a separate and complete offence, no matter the extent to which the information network is involved. These provisions in fact reduce the threshold of criminal offences, and consequently restrict the online freedom and enhance the control over cyberspace in practice.

2.4 Current Legislation on Cybercrime

With two Amendments, the current cybercrime legislation contains cyber offences of illegal access, computer interference, failed in supervising the network, illegal use of the network, and assistance of computer crime.

2.4.1 Illegal access to computer

Illegal access to computer is penalised under Article 285. It contains three subsections, criminalising activities that illegally accessing to the listed computer, illegally changing data or controlling a computer after accessing it, and providing tools that can be used to conduct previous activities.

2.4.1.1 Illegal access to the listed computer information system

Illegal access to the listed computer is penalised under Article 285(1). It rules that 'whoever violates state regulations and secures access into computer information systems concerning state affairs, national defence, and sophisticated science and technology' shall be pursued criminal liability.[195] Four elements can be observed from the wording of this offence: (1) computer information system; (2) involved in state affairs, national defence and sophisticated science and technology; (3) secure access; and (4) in violation of the State's regulations.

Firstly, although in China the public and the academic refer to relevant offences as 'computer crime', the subject protected by the criminal law is actually the 'computer information system' rather than the 'computer'.[196] However, the CL does not explain what the 'computer information system' refers to. According to the *Interpretation 2011,*[197] the term 'computer

[195] Article 285(1) of the Criminal Law.

[196] As an exception, Paragraph 3 of Article 286 uses the term 'computer system' rather than 'computer information system'. These two terms are interchangeable, according to the Interpretation 2011. See Article 11 of the Interpretation of the SPC and the SPP of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems 2011, *Fa Shi* [2011] No. 19.

[197] Interpretation of the SPC and the SPP of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems 2011, *Fa Shi* [2011] No. 19.

information system' refers to 'a system with an automatic data processing function, including computers, networking equipment, communication equipment, and automatic control equipment'.[198] At the same time, another legal instrument - *the Regulation 1994*[199] - also provides a definition of 'computer information system'. The *Regulation 1994* defines it as 'a system composed of computing and supplementary sets of equipment and facilities (including the information network), carrying out collecting, processing, storing, transferring, searching and other operations of information in accordance with specific aims and rules'.[200] Both of these definitions focus on the function of the computer information system regarding data. Given that the *Interpretation 2011* is newly issued and that the Judicial Interpretation of the SPC and the SPP can be used directly as the ruling basis, the definition in the *Interpretation 2011* is adopted when prosecuting and adjudicating cases.

Secondly, analysing elements (2) and (3) together, it can be seen that merely securing access to the computer information system involved in the listed fields constitutes a criminal offence, without the offender performing any further action such as copying or deleting data stored on the computer. In other words, mere hacking to the listed computer information systems without causing any material harm is criminalised under this Article.

Thirdly, the adoption of 'in violation of the State's regulations' leads to an incredibly large number of laws and regulations for judges to interpret.[201] The term 'in violation of the State's regulations' is a term commonly used in Chinese criminal law, intended to enhance the consistency between the criminal law and other laws and regulations. However, what 'State's regulation' means is unclear. According to Article 96 of the CL, 'State's regulations' refers to the laws and regulations issued by the NPC, the SCNPC and the SC. In this sense, all of the laws and regulations issued by these three institutions fall into the category of 'State's regulations'. That means, to keep the consistency among judgements, judges need to

[198] Article 11 of the Interpretation of the SPC and the SPP of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems 2011, *Fa Shi* [2011] No. 19.

[199] Safety and Protection Regulations for Computer Information Systems 1994, *Decree No. 147 of the State Council*.

[200] Article 2 of the Safety and Protection Regulations for Computer Information Systems 1994, *Decree No. 147 of the State Council*.

[201] For discussion of the term 'in violation of State's regulations', see e.g. Zhang Jianjun, '论空白罪状的明确性' (An Analysis on the Clarity of Blank Elements of Criminal Offences), *Faxue* (Legal Science), 5(2012): 139-148; see also Tu Longke and Qin Xincheng, '空白罪状补充规则的适用' (The Application of Blank Elements of Criminal Offences as Supplement), *Faxue* (Legal Science), 10(2011): 153-160.

consider the CL and its Amendments, Judicial Interpretations, guiding cases, and even administrative regulations when adjudicating computer cases.

2.4.1.2 Illegal changing of data stored on a computer information system and illegal control over a computer information system

Article 285(2) penalises the activities of deleting, amending or adding the data stored on or controlling a computer information system after gaining access to it. It is deemed as a step forward on the basis of Article 285(1) to protect computers belonging to individuals and companies. In addition, Article 285(2) criminalises the further activities after gaining access, rather than hacking itself. Therefore, mere hacking to personal computer information systems is not a criminal offence. This wording indicates that the security of data stored on personal computers is not a separate interest; rather, it is based on the security of the personal computers.

However, the rationales reflected by the wording suggest that the security of data and the security of computer are protected for different reasons. For the case of computer, the prohibition of illegal control over a computer information system reflects the protection of the owner's right over the computer. In other words, the computer is regarded as property under this offence. The definition of 'computer information system' focuses on the function of a computer information system also reflects the rationale of treating computer as property.[202] For the case of data, Article 285(2) proscribes deleting, amending or adding data after gaining access to computers. It indicates the protection of the reliability of any data stored on a computer.

Therefore, Article 285(2) does not explicitly state or distinguish the specific interests it intends to shed light on.

2.4.1.3 Providing special tools for illegal access, illegal obtaining of data and illegal control over computers

Article 285(3) mainly deals with the situation where an actor provides programs or tools which can be used for the offences under Article 285(1) and (2), or where the actor knows that another person intends to hack or control a computer information system illegally, but

[202] Yu Zhigang, '网络空间中帮助使用盗窃行为的实行化' (The Online Activities Assisting Theft), *Guizhou Minzu Xueyuan Xuebao (Zhexue Shehui Kexue Ban)* (Journal of Guizhou University for Ethic Minorities (Philosophy and Social Science)), 6(2009): 100-108.

still provides this person with such programs or tools. Generally speaking, the offence under Article 285(3) regulates the preparation and aiding of computer crime.[203] One of the reasons for Article 285(3) is that with the assistance provided by the programs or tools, anyone, even those without a professional background in computer technology, could gain access to the computers belong to others.[204] Another reason is that obtaining such tools is easy due to the increased popularity of the Internet.[205] For example, the amounts of the 'students' in one online hacker school are more than one million, from which they could purchase malicious programs and assistance.[206] Such situations make the criminalisation of disseminating malware that can assist with computer crime necessary.[207]

However, the so-called dual-purpose tools raise issues. 'Dual-purpose' tools refer to the tools or programs that both can be used to test the security of software by the specialists and can be used by hackers to commit computer crime. As explained in the *Interpretation 2011*,[208] the 'special programs or tools' prohibited under Article 285(3) are those programs or tools that have no other purpose than gaining access to or controlling computer information systems.[209] A judge of the SPC has suggested that when interpreting this term, on the basis of Article 2 of the *Interpretation 2011*, three elements must be taken into account: 1) as with the *actus reas* of Article 285(2), the program or tool must have the primary function of obtaining data stored on a computer information system or controlling a computer information system; 2) the program or tool has the capability to circumvent or break through the security measures of the computer information system; and 3) the obtaining of data or control over the computer

[203] Mi Tienan, '共犯理论在计算机网络犯罪中的困境及其解决方案' (The Dilemmas and Solutions of Accomplice Theories in the Context of Computer Crimes), *Jinan Xuebao* (Jinan Journal), 10(2013): 53-63.

[204] Yu Zhigang, '网络空间中培训黑客技术行为的入罪化' (The Criminalisation of Training Hackers in Cyberspace), *Yunnan Daxue Xuebao Faxue Ban* (Law Edition Journal of Yunnan University), 1(2010): 86-95.

[205] *Ibid*.

[206] See more details on '中国黑客学校：百万会员，获千万风投' (Chinese Hacker School: 1 Million members, and 10 Million RMB Venture Investment).

[207] '刑法最新修正案为计算机网络信息系统等新型犯罪定罪' (The newest Amendment to the Criminal Law Provides Ruling Basis for Computer Information Crimes), *Lawtime.Cn*, 1 April 2009, available at http://www.lawtime.cn/info/xingfa/xfnews/2009040136806.html. Last visited March 2013.

[208] Interpretations of Several Issues on the Application of Law in Handling Criminal Cases about Endangering the Security of Computer Information Systems 2011, *Fa Shi* [2011] No. 19.

[209] Article 2 of the Interpretation of the SPC and the SPP of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems 2011, *Fa Shi* [2011] No. 19.

information system can be conducted without rights.[210] Elements 2) and 3), suggested by this judge, distinguish between the dual-purpose tools and those which are solely malicious.[211] According to him, the dual-purpose tools used by specialists to test the security of computer information systems do not normally possess both characteristics listed and defined under 2) and 3). They have either the capacity to breach a security system or a data stealing function; yet malicious programs always include these two functions. Taking this opinion into consideration, the dual-use tools are not prohibited.[212] However, there seems to be a loophole in this reasoning. Possessing both the functions described in 2) and 3) may mark the difference between the dual-use programs and the malicious programs, but this does not necessarily mean that a program which does not satisfy 2) and 3) at the same time is not malicious, and should thus not be prohibited. Some testing tools may also have multiple functions. Besides, these elements are generalised on the pre-requisite that the dual-purpose programs are legal, yet neither the CL nor the *Interpretation 2011* shed light on this very issue. Although, admittedly, the wording of Paragraphs (1) and (2) of Article 2 of the *Interpretation 2011* implies the legal position of the dual-purpose programs implicitly through stressing the above mentioned elements 2) and 3), Paragraph (3) of Article 2, which covers 'other special programs or tools', weakens this implication.

2.4.2 Computer interference

Article 286 penalises activities that delete, amend, add to or disturb the functions of a computer information system, prevent the computer information system from working normally, delete, amend or add to the data or application programs stored, processed or transferred in a computer information system, or make or disseminate programs with these functions, such as a computer virus. The protection of the computers' ability to work indicates the previously mentioned rationale behind the definition of a 'computer information system': the computer information system is protected because it has the function of processing data.

---

[210] Yu Haisong, '《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》的理解与适用' (The Understanding and Application of Interpretation of the SPC and the SPP of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems), *Renmin Sifa (Yingyong) (*People's Judicature (Application)), 19(2011): 24-32.

[211] *Ibid.*

[212] *Ibid.*

Judges' interpretation of Article 286 also echoes with this rationale, as the following case demonstrates.

Case 2.3: Ni Shanlin Case, Jiangsu Province, 25/12/2001[213]

> Ni Shanlin, the accused, installed a program in the system of the network analysis program HPE5100A that turned the screen black when a certain requirement was met, and he set a time-point as his requirement. If the network analysis program ran up to the time-point Ni had set, the screen would turn black. From 1997 to 1999, to further his career, Ni set several of these time points and then fixed the black screens. When he resigned from the company, he did not tell the company about his program, and no one could solve the problem when it happened again. Such settings resulted in huge losses for the company. Prosecutor charged Ni with damaging computer information system so as to cause it unable to work.

During the trial, the main arguments were around the connotation of 'computer information system' as prescribed by the Regulations 1994.[214] The defence lawyer argued that the network analysis program formed no part of a computer information system. But the court rejected this argument by emphasising that the network analysis programs *had the capability to process data automatically*, which made it a computer information system.[215] In addition, since Ni had interfered with such a computer information system, he had committed an offence under Article 286. This reasoning reflected the fact that possessing the capability of automatic data processing is a defining requirement of a computer information system, and thus Article 286 focuses on the function of a computer information system.

2.4.3 Criminal liability of network service providers

Article 286A establishes criminal liability for network service providers in cases where they have failed to perform their supervisory obligations and refused to make corrections when ordered to do so by the regulatory authorities. Before such criminal liability can be pursued, the failure or refusal to fulfil obligations must have resulted in '1) illegal information spreading widely; or 2) a leakage of network users' information that has led to serious

---

[213] *Ni Shanlin Case,* [2001] 锡刑终字第 213 号 (Xixingzhongzi [2001] No. 213).

[214] At that time the Interpretation 2011 had not been issued, so the judges applied the definition of the computer information system in the Regulation 1994 when hearing relevant cases.

[215] *Ni Shanlin Case,* [2001] 锡刑终字第 213 号 (Xixingzhongzi [2001] No. 213).

consequences; or 3) a loss of criminal case evidence and with serious circumstances; or 4) other serious circumstances'.[216]

The aim of this Article is to ensure that network service providers perform the supervisory obligations laid down in laws and governmental regulations. However, when interpreting this Article, one issue arises on what is the so-called 'supervisory obligation'. Since there is no legal provision on this issue, relevant provisions in governmental regulations contribute to an understanding of it. For instance, the supervisory obligations under *the Decision 2012*[217] include but are not limited to, collecting the information on the users' conduct with the information network, adopting the technology necessary to protect information away from theft or leak, deleting illegal network content and reporting it to the relevant governing bodies.[218] Seemingly not complicated. However, as illustrated in section 2.2 of this Chapter, dozens of governmental regulations are concerning cyber security, and many of them contain supervisory obligations for network services providers, leaving a large amount of obligations for network service providers.

2.4.4 Traditional crimes facilitated by computer

Article 287 covers crimes which concern acts that use a computer as a tool to carry out financial fraud, theft, embezzlement, theft of state secrets, and other criminal activities. This article does not establish a computer offence; rather, it states clearly that such activities will be assessed under the criminal provisions for combating traditional crimes. Thus, it explicitly differentiates between crimes that target a computer information system, and crimes that use a computer as a tool,[219] in other words, the genuine cybercrime and traditional crimes facilitated by a computer. The SPC and the SPP have issued several Judicial Interpretations to further the application of this provision in practice. For instance, in 2013 these two judicial organs issued *the Interpretation 2013*, which rules that cases concerning insult in cyberspace are to be punished under the article criminalising insult.[220]

---

[216] Article 286A of the Criminal Law.

[217] *2012年全国人大常委会关于加强网络信息保护的决定* (Decisions Regarding the Strengthening of Network Information Protection 2012).

[218] Articles 2 – 6 of the Decisions Regarding Strengthening Network Information Protection 2012.

[219] Yu Zhigang, '网络思维的演变与网络犯罪的制裁思路' (The Evolution of Cyber Thinking and the Punishment of Cybercrime), *Peking University Law Journal*, 4(2014): 1045-1058.

[220] Articles 1-3 of the Interpretations on the Application of Law in the Handling of Defamation Cases through the Use of Information Networks 2013, *Fa Shi* [2013] No. 21.

2.4.5 Illegal use of the information network

Article 287A penalises activities which, through the use of an information network, '(1) establish websites or communication groups principally for the purpose of committing illegal or criminal activities such as fraud, teaching others how to commit a crime, producing or selling prohibited or controlled articles; (2) disseminating information on the production or sale of drugs, guns, obscene articles, or other prohibited or controlled articles, or illegal or criminal activities; and (3) disseminating information for the purpose of committing fraud, or other illegal or criminal activities.'

Article 287A is inserted in 2015, by the Amendment (IX). It demonstrates a more stringent attitude toward cybercrime in China. Before 2015, criminal liability was pursued if the offender committed the offence using a network or computer. The introduction of a crime committed by means of a network can under certain circumstances be regarded as emphasising the harmful essence of such crime. However, under Article 287A criminal liability is attached not only to the use of a network to disseminate *criminal information*, but also to disseminate *illegal information*. This will result in a situation that in the offline world, the actor who disseminates illegal content may be violating civil or administrative laws; in the online world, however, he is violating the criminal law.[221] It is thus clear that under this Article, the involvement of a network reduces the threshold of criminal liability. In other words, the mere involvement of the network turns a wrongdoing in the offline world into a crime in the online world. Admittedly, the potential harm of online wrongdoing is severe. But such likelihood cannot justify the discrimination between wrongdoings in the online world and the real world; this leads to online/offline inconsistency and over-incrimination.[222]

2.4.6 Ancillary liability – aiding and abetting

Article 287B attaches complete criminal liabilities to ancillary activities that provide technology or other support which will help others to commit crimes through a computer network. To be more specific, if an actor obviously knows that the person to whom they are providing help intends to commit a crime by means of a network, they are violating this provision. Such help includes providing 'internet access, server custody, network storage,

[221] See Li Xiaoming, '刑法："虚拟世界"与"现实社会"的博弈与抉择-从两高"网络诽谤"司法解释说开去'(Criminal Law: Balancing 'the Virtual World' and 'the Real World' – From the Perspective of Interpretation of the SPP and SPC on 'Cyber Insulting'), *Falv Kexue* (Science of Law), 2(2015): 119-131.

[222] *Ibid.*

communication transmission or any other technical support, or providing advertising, payment settlement or any other assistance'.[223]

2.4.7 Jurisdiction

As was indicated previously, provisions dealing with cybercrime are in the CL, meaning that there is no particular jurisdiction principle for cybercrime, and the jurisdiction principles for the CL apply. The jurisdiction principles include territorial principle, nationality principle, protective principle, and universal principle.[224] Among these four, the territorial principle performs as the main principle. It is ruled under Article 6 of the CL that the CL applies to anyone who commits a crime within the territory of the People's Republic of China, except as otherwise provided by law. This Article further states that if a criminal act or its consequence takes place within the territory of the People's Republic of China, the crime shall be deemed to have been committed within the territory of the People's Republic of China. The rider 'otherwise provided by law' refers to situations where a foreigner who enjoys diplomatic privileges and immunities commits a crime in China.[225]

The nationality principle means that the CL applies to any Chinese national who commits a crime outside the territory of the People's Republic of China.[226] The protective principle means that China can claim jurisdiction over any foreigner or any of its own nationals who commit a crime against the State of the People's Republic of China, and that this crime is punishable by no less than three years' imprisonment under the CL, even if the perpetrator is outside the territory of the People's Republic of China.[227] The universal principle means the CL applies to those crimes stipulated in international treaties which have been concluded or acceded to by the People's Republic of China and over which the People's Republic of China exercises criminal jurisdiction within the scope of obligations it agrees to perform.[228]

---

[223] Article 287B of the Criminal Law.

[224] Pi Yong, '关于中国网络犯罪刑事立法的研究报告' (Report on China's Criminal Law on Cybercrime), *Xingfa Luncong* (Criminal Law Review), vol. 27 3(2011): 198-257, pp. 220-222.

[225] Article 11 of the Criminal Law. See also Pi Yong, '关于中国网络犯罪刑事立法的研究报告' (Report on China's Criminal Law on Cybercrime), *Xingfa Luncong* (Criminal Law Review), vol. 27 3(2011): 198-257, p. 220.

[226] Article 7 of the Criminal Law.

[227] Article 8 of the Criminal Law.

[228] Article 9 of the Criminal Law.

Although appearing comprehensive, these four principles are not as effective in cyberspace as they are in the offline world. The territorial principle, nationality principle, and protective principle have all been established on the basis of territory, either inside or outside.[229] However, physical territory no longer exists in cyberspace, so these three principles of determining jurisdiction have little value in cyberspace.[230] In judicial practice, the place where a cybercrime happens is where the commission of the criminal act took place; this includes uploading, downloading and any other operations of the computer information system concerned.[231] If such an operation has taken place in China, China can claim jurisdiction. In addition, if a cybercrime takes place outside of China, if it has had an impact on computers located in China, China can also claim jurisdiction under the protective principle.[232] Reading these two situations together, this principle can be interpreted either in a very broad manner or in a very restricted manner. To be specific, to what extent can an impact qualify as 'having an impact on computers located in China'. Given that almost all computers are connected to the Internet, the electronic signal from a hacking offence launched in the US and targeted at a computer in Singapore may go through a Chinese information highway. Does this qualify as having 'an impact on computers located in China'? If so, there can be hardly any cybercrime over which China does not have jurisdiction. If not, the issue becomes: what does 'has impact' mean? Does it mean the place where the offence was committed, or where the targeted computer was located, or something else? The issue subsequently comes back to the initial question: how to decide where a cybercrime has taken place.

One Judicial Interpretation regarding copyright jurisdiction conflicts between local courts may help. *The Interpretation 2012*[233] adopts the territorial principle, suggesting that the court in the place where the infringement happened or the defendant lives shall have jurisdiction.[234] Further, to solve the problem raised by the lack of borders in cyberspace, the place where the

---

[229] See e.g. Chen Jiemiao, '关于我国网络犯罪刑事管辖权立法的思考' (China's Legislation on Jurisdiction over Cybercrime), *Xiandai Faxue* (Modern Law Science), vol. 30 3(2008): 92-99, p. 93.

[230] *Ibid.*

[231] *Ibid.*

[232] *Ibid*.

[233] Interpretations on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks 2012, *Fa Shi* [2012] No. 20.

[234] Article 15 of the Interpretations on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks 2012, *Fa Shi* [2012] No. 20.

infringement happened refers to the place where the network server, computer terminals or other devices were located.[235] However, this *Interpretation* was issued by the SPP as an instrument to determine jurisdiction in tort cases, and whether such principle applies to cybercrime has not yet been clarified.

The universal principle shows drawbacks as well. Before the universal principle applies, two prerequisites must be satisfied, which hinders the application of the universal principle. The two prerequisites are firstly the activity in question must violate the criminal law in both countries, i.e. dual criminality, and secondly, the countries involved must have participated in or signed relevant international treaties.[236]

Summarising the cybercrime legislation both in the history and in the present, the approach it takes has undergone a significant change in 2015. Previously, legislation on cybercrime focused on the 'computer information system', and protected it from being manipulated, as well as protecting data from being damaged. More recently, the word 'information network' has gained popularity, and the newly introduced offences are either preparing or assisting in crimes conducted in the information network, or the network service provider has failed to supervise the information network. Thus, it seems that 'information network' has replaced the word 'computer information system' and become the new focus of the criminal law. However, according to the definition of 'computer information system', the computer information system actually includes network equipment.[237] Therefore, this shift in the subject of the criminal law appears less necessary. More importantly, as summarised in the historical review, the new approach confuses the 'two points and one dimension' approach set out in the Criminal Law 1997 and *the Decision 2000* of the SCNPC.[238] In addition, actors preparing for or assisting in cybercrime used to be accomplice and could get a less severe punishment compared with the offenders, and the liability of Internet service providers on supervising the information network used to be civil.[239] Under the new approach, the involvement of the

---

[235] *Ibid.*

[236] *Ibid.* See also Yu Zhigang, '关于网络空间中刑事管辖权的思考' (Criminal Jurisdiction in Cyberspace), *Zhongguo Faxue* (China Legal Science), 6(2003): 102-116.

[237] Article 11 of the Interpretation of the SPC and the SPP of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems 2011, *Fa Shi* [2011] No. 19.

[238] *2000 年全国人大常委会关于维护互联网安全的决定* (National People's Congress Standing Committee Decision concerning Preserving Computer Network Security 2000).

[239] For the civil liability of the Internet service providers, see e.g. *2012年最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定* (Provisions of the Supreme People's Court on Several

information network becomes the reason that treating the preparation and assistance of crimes and civil offence as complete crimes.

2.5 The Scope of Cybercrime

The scope of cybercrime has always been a hot topic since it first arose in China, and the CL and its Amendments have not provided a clear answer to this issue yet. In this context, scholars hold differing opinions on this very issue. This section firstly presents three different opinions on the scope of cybercrime, and secondly discusses the contradictive judgements based on different understandings of this issue.

2.5.1 Three opinions on determining cybercrime

One broad opinion on determining cybercrime is that it consists of activities, by making use of the computer and information technology, damaging either the computer data or the network of the State, the community or an individual.[240] This definition is criticised as being too broad to contain at least two subgroups. Firstly, any offence that takes advantage of a computer or its technology can be a computer crime, such as embezzlement through a computer and Internet. Secondly, any crime against computer data and the network of the State, the community or an individual can be a computer crime; such as deleting or forwarding the data stored on a computer and therefore paralysing the network.[241] This definition makes no distinction between the new computer crime and the traditional crime facilitated by computers.[242] The promulgation of Article 287 of the CL 1997 directly refutes such a broad definition.

A narrow definition is that computer crimes are those, using computer technology as their instrument, committed by the unauthorised operation of a computer to destroy the computer

---

Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks), *Fa Shi* [2012] No. 20. See also *2014年最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定* (Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Cases involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks), *Fa Shi* [2014] No. 11.

[240] Jiang Ping, '计算机犯罪初探' (Exploring Computer Crime), *Policing Studies*, 4(1995): 33-36, 25, pp. 33-34.

[241] Zhang Xiuping, '计算机犯罪及其刑法调控' (Computer Crime and Its Legal Regulation), *Journal of Law Application*, 10(1995): 6-8.

[242] *Ibid.*

system.[243] Three constitutive elements can be identified under this definition: 1) the offender had no right to operate the computer, which means that the offence operating a computer without authority should be written explicitly in law; 2) the offender must have destroyed the computer system, which means that different kinds of computer crime have the same criminal target – the computer information system; and 3) the offender has used computer technology as an instrument, which would exclude some conventional crimes such as stealing the hardware of a computer.[244] Admittedly, the scope set by this definition is quite similar to that set by Articles 285 and 286 of the Criminal Law 1997. However, as the Amendment (VII) to the CL have shown, this scope is relatively narrow, and fails to cover some of the newer forms of computer crime, such as DoS attack and the activities damaging data stored on computers.

Some scholars argue that *the Decision 2000*[245] has in fact divided computer crime into six categories,[246] which can be deemed to reflect the SCNPC's opinion as to the scope of computer crime.[247] However, this argument is less convincing. Although the *Decision 2000* lists several so-called *actus reas*, these *actus reas* contains different levels of offences, including criminal offences, administrative offences and civil offences. As Articles 1-5 of the *Decision 2000* state: if the activities are serious to a certain extent and have violated criminal law, relevant criminal provisions should be applied. The term 'relevant criminal provisions' does not necessarily mean provisions concerning computer crime. In addition, category (6) clearly states when infringements are not regarded as severe enough to violate criminal law while violated administrative law or civil law, administrative liability or civil liability shall be pursued.[248] Evidently, civil or administrative wrongdoings cannot be categorised as crimes. Therefore, their observation is untenable in the sense of the statutes.

---

[243] Yang Weiguo, '计算机犯罪立法有关问题初探' (Computer Crimes and Its Relevant Legal Issues), in *The Proceedings of the 11th National Computer Security Conference*, Beijing: China Academic Journal Electronic Publishing House, 1996, pp. 30-34.

[244] *Ibid*.

[245] *2000年全国人大常委会关于维护互联网安全的决定* (National People's Congress Standing Committee Decision concerning Preserving Computer Network Security 2000).

[246] For the details of this categorisation, see section 2.2 of Chapter 2 Cybercrime Legislation in China.

[247] Bin Liang and Hong Lu, 'Internet Development, Censorship, and Cyber Crimes in China', *Journal of Contemporary Criminal Justice,* vol. 26 1(2010): 103-120, pp.112-113.

[248] See more details on *2000 年全国人大常委会关于维护互联网安全的决定* (National People's Congress Standing Committee Decision concerning Preserving Computer Network Security 2000).

2.5.2 The effect of different opinions in judicial practice

Apart from the discussion on the definition and categorisation of cybercrime, Chinese scholars and judges face the other issue with respect to the scope of cybercrime. That is, for instance, an actor hacked a computer, and by the information he obtained from hacking, he committed a traditional offence, such as blackmail. In a situation like this, whether cyber offence encompasses the subsequent traditional crime is under heated debate. To be specific, the number of offences the actor committed is one or two. If the answer is one, it indicates that cyber offence encompasses traditional offence, or traditional offence encompasses cyber offence. In either case a broad way of understanding cybercrime is reflected, since there is no essential difference between cyber offence and traditional offence. If the answer is two, then cybercrime under the CL only refers to the genuine cybercrime, and has a substantial difference from traditional crime – it reflects a narrow way of understanding cybercrime.

A broad understanding of cybercrime is demonstrated in, for example, the case *Chen Xiahui and Zhang Jianfeng Interfering Computer Information System,* where the suspects obtained money by blackmail after hacking into a computer information system. They are convicted of one offence under Article 286.

Case 2.4: Chen Xiahui and Zhang Jianfeng Case, Fujian Province, 05/09/2003[249]

> Chen Xiahui logged into the *Management System of the Traffic Police of Fujian Province* (hereafter the System) and deleted some information stored on the System. Once he knew that he could do this, Zhang Jianfeng worked together with Chen and also deleted some records of traffic violations in the System, charging the violators concerned for this illegal 'service'. Zhang was in charge of searching for violators and collecting the 'fee'; Chen took charge of deleting and amending the violation records. The offenders were convicted of a cybercrime under Article 286.

A narrow understanding of cybercrime can also be observed from judgements. For instance, in the *Li Yong* case, the offender was convicted of two offences, interfering a computer information system and blackmail, on similar grounds of case 2.4.

Case 2.5: Li Yong Case, Shanghai City, 19/03/2010[250]

---

[249] *Chen Xiahui and Zhang Jianfeng Case,* [2003] 丰刑初字第 183 号 (Fengxingchuzi [2003] No. 183).

[250] *Li Yong Case,* [2010] 青刑初字第 117 号 (Qingxingchuzi [2010] No. 117).

> In June 2009, Li Yong logged into a computer information system and created an administration account by means of which he illegally logged into a web-server and deleted all the data stored on that device. He then replaced the homepage of that website with the information: 'this website has a number of security vulnerabilities, please contact me to remedy them.' After recovering the original data, the accused asked for money from the website operator. The accused repeated this process on several other websites and blackmailed the owners for thousands of RMB. He was convicted of two crimes: destroying a computer information system and blackmail.

The inconsistency between the two cases 2.4 and 2.5 illustrates the question on how to assess hacking in preparation for the commission of other intended offences, particularly in a context where the cybercrime provisions do not mention the purpose of facilitating further offences. Since the case 2.4 went to trial in 2003 and the case 2.5 seven years later, it would be reasonable to assume that something might have happened in the period from 2003 to 2010 and had changed judges' position towards such activities. However, in a case that came to trial in 2009, the offender was also convicted of one offence - interfering the computer information system.[251]

Some judges maintain that two offences have been committed. Firstly, the offender hacked into the computer information systems and damaged their function, meaning the systems were unable to function, which violates Article 286. Secondly, for the purpose of illegal gain, the offender asked for money by threatening to destroy others' websites permanently, which violates Article 274. Therefore, the offender had committed two separate offences.[252] When the SPC cited the case 2.4 as a good example of recommended conviction, it was expected that the discussion surrounding this issue would come to an end.[253] Under this interpretation, cybercrime refers to the genuine cybercrime only, and the subsequent activities violating traditional articles should be assessed separately.

---

[251] *Hu Mou and Li Quan Case*, [2009] 虎刑初字第 0363 号 (Huxingchuzi [2009] No. 0363). In this case the two offenders destroyed the network server of an Internet game company, and blackmailed the company for virtual currency that could be used in the Internet game. They were convicted of interfering the computer information system.

[252] *Li Yong Case,* [2010] 青刑初字第 117 号 (Qingxingchuzi [2010] No. 117).

[253] Zhongguo Yingyong Faxue Yanjiusuo of the SPC (China Institute of Application of Law of the SPC), '人民法院案例选' (Example Cases of People's Court), 3(2010).

Other judges support one offence on the basis that although the offender has violated two articles, the activities were conducted for a single purpose – to extort money, which makes the relationship between blackmail and hacking the aim and method. Since a more severe punishment is attached to the interference of a computer information system than to blackmail, it is more appropriate to convict the offender of cybercrime.[254] For instance, in the 2009 case, the judges admitted that two offences had been committed: the preparation carried out by the offenders constituted the offence of interfering a computer information system, yet the facilitated activity constituted blackmail. However, these two offences were conducted for the same purpose. Therefore, given that the punishment attached to interfering a computer information system is more severe than that attached to blackmail, the judges convicted the offenders of interfering computer information system.[255]

The Amendment (IX) is a supporter of one offence. It states explicitly that under Articles 286A, 287A and 287B, if actors, while committing offences under these three Articles, also commits other crimes, they 'shall be convicted and punished according to the provision on the crime with heavier penalty'. Nonetheless, the Amendment (IX) does not clarify whether this rationale applies to the genuine cybercrimes under Articles 285 and 286. Therefore, although the Amendment (IX) seems to provide an authoritative approach to understanding the crimes under the three new Articles, whether this approach is binding on hacking to blackmail, i.e. conducting traditional crimes through the commission of the genuine cybercrime, needs further clarification.

2.6 Summary

China has a multi-level regulating system on cyber wrongdoings, with the CL and its two Amendments the basic and principal instruments. Although both of the two Amendments expanded the scope of cybercrime, the reasons for expansions were different. The Amendment (VII) was issued in 2009 to cover the gap that rose together with the increasing popularity of personal computers. After this Amendment, the 'two points and one dimension' approach was established. This approach draws a clear distinction between the genuine computer crime (i.e. the crimes which target the security of the computer information system and the data, offences under Articles 285 and 286) and traditional crimes facilitated by computers (i.e. offences under traditional criminal provisions). In addition, this approach

[254] *Hu Mou and Li Quan Case*, [2009] 虎刑初字第 0363 号 (Huxingchuzi [2009] No. 0363).

[255] *Ibid.*

distinguishes the genuine cybercrimes that not damaging the function of computers from those damaging the function of computers. Moreover, under this approach, mere hacking is criminalised only when the hacked computer information system involved in the State affairs, national defence or sophisticated technology. For computers belonging to individuals and companies, the actor must either have obtained some information from the hacked computer or controlled it in some way, before being held liable for a criminal sentence. With these distinctions and clarifications, the 'two points and one dimension' approach appears to be a systematic approach. During this period, one main drawback is that the protection on data is relying on the protection on the computer.

In 2015, the Amendment (IX) was issued, and showed some changes with respect to the approach. Firstly, the subject of the newly inserted offences is not 'computer information system' but 'information network' – the one in fact has already included by the definition of 'computer'. Secondly, the 'two points and one dimension' approach no longer exists since the genuine cybercrime and traditional crimes are not regarded essentially different under the new Amendment. For instance, the preparation and assistance of traditional crime facilitated by computers are now regarded as complete cyber crime.

The changes in the approach of the CL raise two problems in particular. Firstly, the Amendment (IX) expands the scope of cybercrime to a large degree. For instance, China decides to pursue criminal liability of network service provider when they fail to filter illegal information online when other countries decide not.[256] Secondly, the inconsistency between the Amendment (IX) and the 'two points and one dimension' approach leads to confusions between traditional criminal provisions and cybercrime provisions, and further reduces the possibility for judges to make far-reaching interpretations.

---

[256] For instance, section 230 of the Communications Decency Act of the United States (47 USC § 230) rules that

'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider'.

Section 26 of Electronic Transactions Act (Chapter 88) of Singapore also rules that

'(1) a network service provider shall not be subject to any civil or criminal liability under any rule of law in respect of third-party material in the form of electronic records to which he merely provides access if such liability is founded on — (a) the making, publication, dissemination or distribution of such materials or any statement made in such material; or (*b*) the infringement of any rights subsisting in or in relation to such material;

(1A) a network service provider shall not be subject to any liability under the Personal Data Protection Act 2012 in respect of third-party material in the form of electronic records to which he merely provides access'.

One possible reason for the changes in the approach is the politicisation in the field of criminal law. As shown by the fact, the main amendments to the criminal law had already been reflected in the administrative regulations, the departmental rules and Judicial Interpretations. Compared with the CL and its amendments, these regulatory instruments are more vulnerable to political intervention.[257] Due to this politicisation, the worry on social stability and national security drives the legislators to replace the previous approach with a more stringent one so as to enhance the control over cyberspace. For instance, Article 1 of the Cyber Security Law (draft) states that its aim is to protect the cyber security and the national security. In addition, the *Measures for Security Protection Administration of the International Networking of Computer Information Networks (2011 revised)* emphasises that no individual or company shall use a network in a way that endangers state security or threatens public interests.

In sum, during the last two decades, transitions can be noticed within the understandings of cybercrime and the legislative approaches against cybercrime. Within the arena of the criminal law and the Judicial Interpretations, contradictory scenarios can be observed in relation to the position on criminalising the wrongful online activities. Apart from the CL and the Judicial Interpretations, Chinese executive organs have also issued an enormous amount of instruments supplementing the CL, including administrative regulations and departmental rules. Unlike the transitions in the positions reflected in the CL and the Judicial Interpretations, from the beginning the supplementary instruments demonstrate the government's desire to enhance the control over cyberspace.

[257] For the details of how the main amendments to the criminal law have been reflected in the administrative regulations, the departmental rules and Judicial Interpretations, see section 2.2 of this Chapter.

Chapter 3 The Convention on Cybercrime of the Council of Europe

3.1 Introduction

The challenges presented by cybercrime appear to be a key task not only for individual nations but also for regional and international organisations. In this context, the Council of Europe (hereafter the CoE) has played an important role in harmonising the criminal law on cybercrime through drafting and promulgating the Convention on Cybercrime (hereafter the CoC or the Convention).[258] The Convention was opened for signature in Budapest, on 23 November 2001 and entered into force on 1 July 2004, with five ratifications including at least three member States of the Council of Europe.[259] By the time of April 2016, the CoC has attracted 48 ratifications and 6 signatures.[260]

3.2 starts with a historical review on the endeavours made by the CoE, intending to unveil the considerations towards an international legal instrument on cybercrime. 3.3 subsequently analyses the terms and offences under the CoC with respect to substantive criminal provisions and jurisdiction. In the end, 3.3 summarises what has been found in 3.2 and 3.3 and generalises the characteristics and the legislative approach of the CoC.

3.2 Historical Review of the Endeavours by the Council of Europe

The lack of protection against cyber wrongdoing from criminal law raised new legal issues and challenged the principles of traditional criminal law.[261] These issues and challenges triggered international discussions and responses. The CoE has been making its endeavours ever since the 1970s. From the 1970s to 2001, when the CoC was ready for signatures, it had sponsored and conducted dozens of research programs and seminars discussing measures

[258] See e.g. Shannon L. Hopkins, 'Cybercrime Convention: A Positive Beginning to a Long Road Ahead', *Journal of High Technology Law*, vol. II 1(2003): 101-122.

[259] The Council of Europe, Convention on Cybercrime, European Treaty Series No. 185, available at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Last visited March 2016.

[260] For the details on the ratifications and signatories, please see http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185andCM=andDF=andCL=ENG. Last visited April 2016.

[261] Ulrich Sieber, 'Legal Aspects of Computer-related Crime in the Information Society: COMCRIME-Study', *prepared for the European Commission,* 1 January 1998, p. 24, available at http://www.oas.org/juridico/english/COMCRIME%20Study.pdf. Last visited May 2015.

against cyber wrongdoing. Many issues had been discussed during this period, for instance, the relationship between the so-called cybercrime and traditional crime, the offences that should be introduced to tackle cybercrime, and, the proper way of dealing with the intangible nature of cybercrime. In addition, during this period, scholars have identified six waves of cybercrime legislations, which indicates six fields that cybercrime legislation may shed light on.

3.2.1 Historical review of the CoE efforts against cybercrime

Although the Convention opened to signature in 2001, the efforts of drafting such a legal instrument within the framework of the Council of Europe has long been taken. Generally, the history of the efforts can be divided into three periods, judging from the main issues each period discussed: (1) in the 1970s the efforts were mainly made on using the Economic Crime legislation dealing with 'computer-related crime',[262] (2) in the 1980s the efforts were mainly made on negotiating and preparing for a new and specific legislation on 'computer crime', and (3) in the 1990s the efforts were mainly made on harmonising the procedural criminal law.

3.2.1.1 In the 1970s: tackling 'computer crime' with the economic crime legislation

As early as the 1970s, the Council of Europe had noticed and stressed the international nature of 'computer crimes' and initiated a discussion from the perspective of the economic crimes - the first time the issue of 'computer crime' was discussed within the framework of the CoE.[263] This discussion resulted in one task on the agenda of the CoE – to finish a report on 'computer crime' in the following years.[264] The Recommendation No. R (81) 12[265] proposed by the selected committee on Economic Crime is this report. The Committee of Ministers adopted it in 1981, in which 'computer crime' was listed as 'theft of data, violation of secrets,

[262] Back then the network was not advanced and thus did not play important roles in crimes. Therefore, in that period crimes with computer involved were referred to as 'computer crime'.

[263] The Council of Europe, Recommendation No. R (89) 9 on Computer-related Crime and Final Report of the European Committee on Crime Problems, *Strasbourg* 1990, available at http://www.oas.org/juridico/english/89-9andfinal%20Report.pdf. Last visited May 2015. See also Stein Schjokberg and Amanda M. Hubbard, 'Harmonizing National Legal Approaches on Cybercrime', International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity. *Document CYB/04*. 2005.

[264] Marco Gercke, 'Europe's Legal Approaches to Cybercrime', *ERA Forum,* vol. 10 3(2009): 409-420, p. 415.

[265] The Council of Europe, the Committee of Ministers to Member States on Economic Crime, Recommendation No. R (81) 12, 25 June 1981, available at https://www.coe.int/t/dghl/monitoring/greco/general/R(81)12%20on%20economic%20crime_EN.pdf. Last visited May 2015.

manipulation of computerised data'.[266] As commentated in a later report, this Recommendation pointed at

> 'the non-specific offence which, in the context of recommendation on economic crime, is to be taken into consideration only when it:
>
> i. causes or risks causing substantial loss;
>
> ii. pre-supposes special business knowledge on the part of the offenders; and
>
> iii. is committed by businessmen in the exercise of their professional functions.'[267]

Judging from this comment, one can see that the 'computer crimes' the CoE intended to tackle at that time were the ones causing substantial, or in other words, monetary loss in business. Therefore, the prohibited 'computer crime' in this period was in fact a sub-category of economic crime but not a unique category of crime. In addition, the use of 'computer crime' was just to emphasise the involvement of computer in such crimes.

3.2.1.2 In the 1980s: negotiating and preparing for the substantive criminal law on 'computer-related crime'

As time went by, computer crime gradually became a separate category of crime in the 1980s and was not limited to economic crime anymore. Computer wrongdoings such as hacking emerged, and an increasing number of hacking offences were committed not for economic gains but for fun or for showing off the offender's computer skills. Against this background, the CoE assigned 15 experts as an Expert Committee to discuss the legal aspects of computer crimes in 1985.[268] This time, the term used was not 'computer crime' but 'computer-related crime', arguably intending to cover all crimes with computer involved, no matter hacking, theft of data, or online fraud.

Four years later, the European Committee on Crime Problems adopted the Report of the Expert Committee on 'computer-related crime', i.e. the Recommendation No. R (89) 9, in which substantive criminal provisions were recommended as necessary to fight against computer-related crimes, such as computer-related forgery and fraud.[269] Whilst

[266] The Council of Europe, Committee of Ministers, Recommendation No. R (81) 12, p. 4.

[267] The Council of Europe, Recommendation No. R (89) 9, pp. 11-12.

[268] Marco Gercke, 'Europe's Legal Approaches to Cybercrime', *ERA Forum,* vol. 10 3(2009): 409-420, p. 415.

[269] *Ibid.*

Recommendation No. R (89) 9 analysed the difficulties of combating the new phenomenon of computer-related crime by diverse domestic criminal provisions, it stressed that only a universally binding legal instrument could serve the goal of fighting against this new phenomenon.[270]

Moreover, as one of its conclusions, the Recommendation No. R (89) 9 provided a minimum list of computer-related crimes, consisting of computer-related fraud, computer forgery, damage to computer data or programs, computer sabotage, unauthorised access, unauthorised interception, unauthorised reproduction of a protected computer program and unauthorised reproduction of topography.[271] This list sets out a framework for the future draft of the CoC.

3.2.1.3 In the 1990s: harmonising the procedural criminal law

Considering the issues of search and seizure, electronic evidence, and international cooperation, the harmonisation of procedural law concerning information technology became the main concern in the 1990s. For instance, Professor Kaspersen pointed out, in a report on implementing the Recommendation No. R (89) 9, that '…a Convention… should not only deal with criminal substantive law matters, but also with criminal procedural questions as well as with international criminal law procedures and agreements'.[272] Professor Ulrich Sieber also stressed the importance of cross-border collaboration and especially the harmonised activities between various organisations to combat computer crimes in a report he prepared for the European Commission in 1998.[273] At the national level, Sieber pointed out, the lack of comprehensive and international solutions to computer crime was still perplexing the experts and domestic judges.[274] For instance, the absence of a mutual assistance section made it hard to extradite the suspect. Moreover, considering the need for international investigation in cross-border computer crimes, the lack of a relevant legal instrument would result in the pending of the case.[275]

---

[270] The Council of Europe, Recommendation No. R (89) 9.

[271] *Ibid.*

[272] Henrik W. K. Kaspersen, 'Implementation of Recommendation No. R (89) 9 on Computer-related Crime', Strasbourg, March 1997, *Doc. CDPC (97) 5 and PC-CY (97) 5*, p. 106.

[273] Ulrich Sieber, 'Legal Aspects of Computer-related Crime in the Information Society: COMCRIME-Study', *prepared for the European Commission*, 1 January 1998.

[274] *Ibid*, pp. 3-4.

[275] *Ibid.*

In response to the concerns on the procedural issues, the Committee of Ministers of the CoE adopted the Recommendation No. R (95) 13 on problems of the procedural law with respect to information technology.[276] Apart from adopting this Recommendation, the European Committee on Crime Problems further set up a committee of experts to deal with procedural issues regarding information technology in 1996, which held ten meetings in plenary session and fifteen meetings with its open-ended Drafting Group from 1997 to 2000.[277] During these meetings, the cooperation and mutual assistance between countries and international and supra-national organisations remained the core of the legal solution for combating computer crime.

Apart from the assigned experts, scholars also took part in finding solutions on harmonising the procedural law. For instance, Sieber raised four points for legal measures against computer crime: '(1) the elaboration of a directive on the general (civil and criminal) responsibility of access and Internet service providers; (2) the consideration of a directive which could define legal, illegal and harmful contents in computer networks, which would not only require member states to create effective sanctions against these illegal and harmful contents but also prohibit member states from restricting international data flow with respect to illegal and harmful contents not listed in the directive; (3) the inclusion of a list of illegal acts to be prohibited and covered by adequate sanctions of national law in a future directive in order to guarantee security and consumer protection in European computer networks; and (4) improved information on legal solutions in the member states'.[278] Judging from the contents of the CoC, all of these four points are reflected to some extent in it.

3.2.2 Main discussions behind the CoC

It took the CoE about three decades to discuss and analyse the issues on computer crime and finish the Convention. During this process, three issues were especially discussed regarding the substantive criminal law, including the definition of 'computer crime', the 'victims' and threatened legal interests of computer crime, and the potential of over-criminalisation of an international legal instrument.

---

[276] The Council of Europe, 'Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology', available at http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1995)013_EN.asp. Last visited June 2015. See also Article 10 of the Explanatory Report of the Convention on Cybercrime, available at http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm. Last visited June 2015.

[277] Marco Gercke, 'Europe's Legal Approaches to Cybercrime', *ERA Forum,* vol. 10 3(2009): 409-420, p. 416.

[278] Ulrich Sieber, 'Legal Aspects of Computer-related Crime in the Information Society: COMCRIME-Study', *prepared for the European Commission*, 1 January 1998, p. 6.

Firstly, the question of how to define 'computer crime',[279] or in other words, the elements that making an offence a computer one, raised concerns. As presented in the Introduction Chapter, all the definitions and terms describing the computer and cyber phenomenon lack of clarity. Moreover, the lack of clarity cannot be 'reconciled with the aim of being succinct and precise and leaving no doubts as to the scope or the use of the definition'.[280] Among the different definitions given by different organisations and experts, some of them may be not specific enough and therefore not useful,[281] and others may be so narrow that some misuses of computers were excluded.[282] In this context, concerned about a formal and universal definition may create more troubles than it could solve, and hinder the individual states ratifying the Convention, the experts assigned by the CoE decided to leave the definition to national legislatures.[283] Therefore, in the CoC there was no definition of computer crime/cybercrime, but two lists of offences[284] that was recommended to be criminalised at the national level.

The second issue with respect to substantive criminal law discussed when drafting the CoC was the object of the Convention, or, the subject of cybercrime. The objects protected by the then existing criminal law were all physical and visible, while the interests threatened by various forms of computer crime were not always physical or visible.[285] The interests threatened by computer crime may be divided into two types: the existing legal interests threatened by offences, such as property, and the new kinds of interests emerging together with computerisation, such as the security of computer data. The question of whether both kinds of interests should be protected by the criminal law was under heated discussion.[286] To

[279] The Convention on Cybercrime adopted 'cybercrime'. To keep it consistent with previous discussion, here the author still uses 'computer crime'. These two terms are interchangeable in this thesis as explained in the Introduction Chapter.

[280] The Council of Europe, Recommendation No. R (89) 9.

[281] For instance, the OECD defined it as 'any illegal, unethical or unauthorised behaviour relating to the automatic processing and the transmission of data'. However, the experts assigned by the CoE 'did not find it useful to aim at a more precise definition but chose instead a functional classification'. Recommendation No. R (89) 9, p. 13.

[282] For instance, a writer defined 'computer crime' as 'any illegal action in which a computer is a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the function of a computer' (this definition excluded computer-related fraud and forgery). Recommendation No. R (89) 9, p. 13.

[283] The Council of Europe, Recommendation No. R (89) 9, p. 13. See also Shannon L. Hopkins, 'Cybercrime Convention: A Positive Beginning to a Long Road Ahead', *Journal of High Technology Law*, vol. II 1(2003): 101-122.

[284] The offences under these two lists will be discussed in detail in section 3.3.

[285] The Council of Europe, Recommendation No. R (89) 9, pp. 21-23.

[286] *Ibid.*

be specific, the vast manifestations of computer offences including data theft may be worthy of legal protection, while their difference with traditional offences hindered the extension of criminal law into cyberspace.[287] The core question, therefore, became to what extent a specific interest was worthy of protection, especially to what extent the criminal law should be applied.[288]

To answer this question, one criminal principle should be taken into consideration: the principle that the criminal law should not be invoked unless other techniques are inadequate, in other words, the criminal law should be the last resort. In all types of interests violated by computer crime, certain interests could be selected as deserving further protection against the misuse of information technology; this, however, does not mean the criminal approach should be automatically applied to provide protection.[289] As a principle of criminal law, criminalisation should only be applied when other measures are insufficient and not infringe freedom excessively.[290] Therefore, whether to use criminal law was the resulting question of balancing the competing factors, i.e. online freedom and cyber security.[291]

With respect to this balance, the experts committee of the Recommendation No. R (89) 9 took cyber security as priority, and expressed that 'a combined effort to contain and reduce computer-related crime by a balanced variety of means is necessary, in which criminal law provisions and their enforcement play an important role'.[292] To reach this conclusion, the experts committee must reject, or at least challenge, all the other measures that determining crimes with computer features. This is exactly what they did. According to them, the self-regulating Codes of Conduct with respect to the cyberspace could only restrain the acts of the members of 'professional organisations'; the administrative sanctions might be too limited to provide prevention or/and repression; and a damage claim with civil compensation meant nothing if the damage could not be evaluated in terms of money which was a normal

[287] *Ibid.*

[288] *Ibid*, pp. 21-24.

[289] The Council of Europe, Recommendation No. R (89) 9, p. 24.

[290] Andrew Ashworth and Jeremy Horder, *Principles of Criminal Law* (7th edition), Oxford: Oxford University Press, 2013, p. 33.

[291] See e.g. Roberto Flor and Joon Oh Jang, 'Cyber-criminality: Finding a Balance Between Freedom and Security', in Stefano Manacorda (ed.), *Cybercriminality: Finding a Balance Between Freedom and Security-Selected Papers and Contributions from the International Conference on 'Cybercrime: Global Phenomenon and its Challenges'*, Courmayeur Mont Blanc, Italy, 2-4 December 2011.

[292] The Council of Europe, Recommendation No. R (89) 9, p. 25.

situation in computer crime.[293] Thus, amendments to criminal law in order to make it applicable to computer crimes are necessary.

However, the application of criminal law to computer crime may result in over-criminalisation. The interpretation of criminal law in respect of computer crime inevitably had a vague scope considering the development of technology, and so with cybercrime.[294] Worrying about this, and also about the possibility that new criminal provisions would lead to an overlap with the existing criminal law, the Committee of the Recommendation No. R (89) 9 had considered stretching the then existing criminal law on computer crime in the beginning.[295] Nonetheless, this route was not adequate. The boundaries between extensive interpretation and the prohibited analogy were so vague that in fact the application of current criminal provisions to computer crimes could hardly avoid raising doubts.[296] Considerable uncertainties emerged subsequently. Thus, as argued by Ulrich Sieber, it might be appropriate to close the gaps with the new criminal law, rather than stretching the existing criminal laws by re-interpreting them.[297]

To date, there was no consensus or mainstream view on the issue that to what extent criminal law should apply in the cyberspace. Applying the criminal law to computer crime is to deter and combat it. The deterrence of criminal law is determined by the 'likelihood of being caught, the speed of adjudication and the severity of punishment'.[298] Therefore, this issue should be put into the context of each judicial system, rather than an international legal instrument. Sharing this idea, the assigned experts of the CoE proposed six criteria for framing amendments to the then existing criminal laws. They are

i. the causing of substantial/significant damage or injury;
ii. that the criminalised offences could only be committed by a certain category or type of person, in other words, only those who knew computer techniques could be criminalised;[299]

---

[293] *Ibid*, p. 25.

[294] *Ibid*, p. 26.

[295] *Ibid.*

[296] *Ibid*, p. 27.

[297] Ulrich Sieber, 'Legal Aspects of Computer-related Crime in the Information Society: COMCRIME-Study', *prepared for the European Commission*, 1 January 1998.

[298] The Council of Europe, Recommendation No. R (89) 9, p. 28.

[299] The experts also expressed their concern that these criteria could result in the computer-related criminal law too limited to apply in judicial practice.

iii. the third criterion was about the distinction between offences committed within the computer system and those committed by outsiders. Assessment of this criterion differed from jurisdiction to jurisdiction, while this issue was worthy of consideration;

iv. the objective element of whether or not there were technical devices for the protection or security of computer systems, data banks, programs or data;

v. the form of guilt. In other words, should computer offences with the element of intention be criminalised? Or could other types of *mens rea* also be seen as a constituent element;

vi. the last criterion related to procedural pre-requisites for prosecution in some countries, the difference between the principle of discretionary prosecution and the principle of mandatory prosecution led to different incrimination standards.[300]

3.2.3 The Main Waves of Domestic Cybercrime Legislation

In the Report prepared by Ulrich Sieber, six waves of criminal legislation with respect to computer crime were identified, indicating six potential fields of cybercrime legislation:[301]

(1) Protection of Privacy

This wave started from the 1970s. The data stored, computed and transmitted in electronic devices provided new opportunities for collecting personal information. As a response to these opportunities and to protect personal information, several jurisdictions established relevant laws. The Federal Republic of Germany, for instance, promulgated its Data Protection Act in January 1977 and revised it in 1990, with the United Kingdom in 1987 and the Netherlands in 1988.[302]

(2) Economic Criminal Law

Starting from the beginning of the 1980s, the incidence of computer-facilitated economic crimes surged. Such crimes not only threatened the traditional legal interests like property but also threatened the intangibles like computer data. In this context, when applying the traditional criminal provisions, the subtle boundary between extensive interpretation and analogy presented problems, and the sharp increase in computer-facilitated economic crime

[300] Abstracted from the Council of Europe, Recommendation No. R (89) 9, pp. 30-32.

[301] Ulrich Sieber, 'Legal Aspects of Computer-related Crime in the Information Society: COMCRIME-Study', *prepared for the European Commission*, 1 January 1998.

[302] *Ibid*, pp. 25-27.

presented a real dilemma for the then judicial system. Therefore, the United States of America, as a forerunner, enacted a law against computer-facilitated economic crimes at the national level in 1984, and the Federal Republic of Germany adopted a similar way in 1986.[303]

(3) Protection of Intellectual Property

The third wave of computer legislation related to intellectual property. Since in Europe methods of performing mental acts were not regarded as patentable inventions, the Articles of the European Patent Convention did not shed light on the patentability of computer programs. Most European jurisdictions followed this idea and ruled computer programs out of their national patent legislations. Gradually these jurisdictions realised the importance of protecting the intellectual property of computer programs. Therefore, laws protecting the copyright and other related rights of computer programs were enacted in the 1980s, the Federal Republic of Germany and the United Kingdom in 1985 for instance.[304]

(4) Protection against illegal and harmful contents

In 1980s several jurisdictions started to reform legislation against illegal and harmful digital contents, and this reform developed into a trend in other jurisdictions rapidly in the mid-1990s due to the popularity of the Internet. The measures taken can mainly be generalised in two categories: firstly, amending the traditional legislation on the dissemination of 'pornography, hate speech or defamation to computer data', such as the United Kingdom; secondly, enacting new special provisions clarifying 'the responsibility of service and access providers on the internet', such as the US.[305]

(5) Criminal Procedural Law

In the 1980s, most jurisdictions gradually realised the problem with the lack of procedural rules against computer crime and thus started to reform the procedural criminal law. To be specific, jurisdictions enacted new laws, for instance, the United Kingdom promulgated the Police and Criminal Evidence Act in 1984, and the Netherlands enacted Sections 125 f-n of the Criminal Procedural Code, all to update the criminal procedural law.[306]

---

[303] *Ibid*, pp. 27-28.

[304] *Ibid*, pp. 28-30.

[305] *Ibid*, p. 31.

[306] *Ibid*, p. 31.

(6) Security law

The last wave is the legal reform in the field of the requirements of security measures. This series of laws encompassed 'the minimum obligation for security measures in the interests of privacy rights or in the general public interest'.[307] It also included 'prohibitions of specific security measures in the interest of privacy rights or of effective prosecution of crimes (such as limitations of cryptography)'.[308]

The three decades' discussions on competing factors behind criminalising computer crime laid the foundations of the CoC. The issues discussed during this period, as shown in other Chapters of this dissertation, are reflected to a greater or lesser extent at the national level as well. The CoE's considerations and answers to these issues provide insights for the individual nations in enacting their domestic laws. Moreover, by opening the CoC for signature in 2001, it provides a guideline of cybercrime legislation not only for its member states but also for those non-member states.[309]

3.3 The Offences under the Convention on Cybercrime

Set out in the preamble, the main objective of the CoC is to pursue a common criminal policy to protect society against cybercrime, especially by adopting proper legislation and nurturing multinational co-operation.[310] The main text of the CoC has four major parts, encompassing both substantive and procedural issues.

1. Articles 2 - 13 constitute the substantive part of the Convention. In this Section, a list of recommended offences is provided. In addition, the liability of inchoate crimes and corporates, and appropriate sanctions and measures are also included.[311]
2. Articles 14 - 22 are the procedural part of the Convention. This part outlines the powers law enforcement agencies should be granted when investigating and prosecuting offences under the CoC, including the power to order an Internet Service

[307] *Ibid*, pp. 31-32.

[308] *Ibid*, p. 31.

[309] Amalie M. Weber, 'The Council of Europe's Convention on Cybercrime', *Berkeley Technology Law Journal*, vol. 18 (2003): 425-449, p. 443. See also Alexander Seger, 'The Budapest Convention 10 Years on: Lessons Learnt', in Stefano Manacorda (eds.), *Cybercriminality: Finding a Balance between Freedom and Security-Selected Papers and Contributions from the International Conference on 'Cybercrime: Global Phenomenon and its Challenges'*, Courmayeur Mont Blanc, Italy, 2-4 December 2011.

[310] See more details on 'Convention on Cybercrime-Summary of the Treaty', available at http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm. Last visited November 2013.

[311] The Council of Europe, Convention on Cybercrime, European Treaty Series No. 185.

Provider (hereafter the ISP) to preserve a citizen's internet usage records or other data and to compel a person in its territory to provide specified stored computer data in real time. It ends with the jurisdiction provisions.[312]

3. Articles 23 – 35, the third part of the CoC, sets out guidelines for international co-operation. It requires all the signatories to assist each other where offences prescribed in the substantive part are committed, and 'to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form about a criminal offence'.[313]
4. Finally, Articles 36 – 48 pertain to the effect of the Convention, such as the reservations, the amendments, the disputes settlement, and the withdrawal of the Convention.[314]

With respect to the substantive offences, the drafters prepare a list of offences that signatories must prohibit with their domestic law, including

Unauthorised access without rights that leads to serious harm;

Unauthorised interception: the interception, made without right and by technical means, of non-public transmissions of computer data to, from and within a computer system or network;

Damage to computer data: the erasure, deletion, destruction or suppression of computer data or computer programs without rights and resulting in serious harm;

Damage to a system: the input, alteration, erasure or suppression of a computer system, or other interference with computer systems, with intent to hinder the functioning of a computer system;

Misuse of devices: the selling, distributing or otherwise making available of computer passwords, access code or similar data;

Computer fraud and forgery; and

Producing, offering or distributing child-pornography.[315]

---

[312] *Ibid*.

[313] The Council of Europe, Convention on Cybercrime, European Treaty Series No. 185.

[314] *Ibid*.

[315] *Ibid*.

However, this list is a compromise between different legal systems and traditions and serves as a minimum requirement for being a signatory. The CoC further provides an optional list of offences on which an international consensus is harder to reach, including

> *Unauthorised use of a computer not included in the minimum list*;
>
> *Alteration of computer data without right and resulting in no serious harm*;
>
> *Computer espionage*: producing, selling, distributing or otherwise making available of computer programs that were designed for the purpose of committing unauthorised access, interception and interference of data and systems;
>
> *Procuring or possessing Child-pornography*; and
>
> *Infringements of copyright and related rights*.[316]

The substantive part includes four categories. Articles 2 - 6 criminalise 'offences against the confidentiality, integrity and availability of computer data and systems', in which data and computer system are the targets. The second category contains Article 7 and Article 8, prohibiting 'computer-related crime', namely, computer facilitated forgery and fraud. The third category is 'content-related crime', outlawing making, uploading, distributing, procuring and possessing child pornography and related crimes. The fourth category introduces offences related to infringements of copyrights and related rights.

Generally speaking, the criminal offences prescribed under the CoC share two constitutive elements: one is 'without right', and the other one is 'intentionally'. The former refers to the situation where 'conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law',[317] and the signatories can determine how to interpret this element considering their domestic legal system,[318] as suggested in the Explanatory Report of the CoC (hereafter the ERCoC). The latter is a constituent element for all offences under the CoC, except

[316] The Council of Europe, Convention on Cybercrime, European Treaty Series No. 185.

[317] Article 38 of the Explanatory Report of the Convention on Cybercrime.

[318] *Ibid*.

infringement of copyright and related rights.[319] Both of these two elements perform as filter tools in order to avoid over-criminalisation.[320]

3.3.1 Terms used in the CoC

Article 1 of the CoC defines four important terms: 'computer system', 'computer data', 'service provider' and 'traffic data' – the ones that constitute the foundation of offences. Nonetheless, the signatories of the CoC do not need to copy these definitions into their domestic law, as suggested in the ERCoC.[321] Instead, they can develop their own definitions, 'provided that these laws cover such concepts in a manner consistent with the principles of the Convention and offer an equivalent framework for its implementation'.[322]

According to Art. 1 of the CoC, the 'computer system' refers to 'any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.' In the ERCoC, this term is further explained as 'a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities'.[323] According to the definition and explanation, the CoC protects a computer system's capability of processing data. It thus holds true that the computer system in the CoC is not just virtual equipment without value, but a tangible object with specific capability, and thus, with value. In other words, the CoC treats a computer system as useful property and thus protects it.

'Computer data' is defined as 'any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function'. The drafters further explained in the ERCoC that data is 'a form that can be directly processed by the computer system', or in other words, is electronically or by other means directly processable.[324] It is worth pointing out that computer data for the purpose of the CoC is regarded as one of the targets of computer

[319] Article 113 of the Explanatory Report of the Convention on Cybercrime.

[320] Mike Keyser, 'The Council of Europe Convention on Cybercrime', *Journal of Transnational Law and Policy*, vol. 12 2(2003): 287-326, p. 299. The author regards the element of 'intentionally' as 'important to filter the number of offenders and to distinguish between serious and minor misconduct'.

[321] Article 22 of the Explanatory Report of the Convention on Cybercrime.

[322] *Ibid*.

[323] Article 23 of the Explanatory Report of the Convention on Cybercrime.

[324] Article 25 of the Explanatory Report of the Convention on Cybercrime.

offences,[325] and the CoC outlaws acts damaging it. Moreover, unlike the protection for a computer system, computer data is not protected because it has capabilities, but because it is electronically or by other means directly processable, and through being processed can deliver information.[326] To be clearer, computer system and data are in fact different elements under the CoC: the former has the capability to process, compute and store the latter.

'Service provider' encompasses a wide category of 'public and private entities that provide to users of their service the ability to communicate by means of a computer system'.[327] According to this definition, its scope is further extended to include those entities that 'process or store computer data on behalf of such communication service or users of such service',[328] no matter it provides its service to the public or to a closed group.[329]

The fourth term 'traffic data' is referring to 'any computer data relating to a communication by means of a computer system, generated by a computer system that forms part of the chain of communication, indicating the communication's origin, destination, route, time, data, size, duration, or type of underlying service'.[330] This definition has raised two concerns. Firstly, the Convention makes ISPs responsible for the preservation of data in case of investigation and prosecution, including the traffic data. This responsibility may result in additional costs for the ISPs.[331] Secondly, the collection of evidence or the identification of the suspect may infringe individual rights, the right to privacy specifically.[332] For a better understanding of the CoC with respect to these concerns, the ERCoC has contributed to clarify this issue. According to Article 29 of the ERCoC, the drafters intended that the collection of data or other investigating measures be done as unobtrusively as possible.[333] Therefore, while they

---

[325] *Ibid*.

[326] Mike Keyser, 'The Council of Europe Convention on Cybercrime', *Journal of Transnational Law and Policy*, vol. 12 2(2003): 287-326, p. 298.

[327] Article 1 of the Convention on Cybercrime, the Council of Europe.

[328] Article 1 of the Convention on Cybercrime, the Council of the Europe.

[329] Article 26 of the Explanatory Report of the Convention on Cybercrime.

[330] Article 1 of the Convention on Cybercrime, the Council of the Europe.

[331] See e.g. Albert I. Aldesco, 'The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime', *Loyola of Los Angeles Entertainment Law Review*, vol. 23 (2002): 81-123. See also Mike Keyser, 'The Council of Europe Convention on Cybercrime', *Journal of Transnational Law and Policy*, vol. 12 2(2003): 287-326, p. 298.

[332] Mike Keyser, 'The Council of Europe Convention on Cybercrime', *Journal of Transnational Law and Policy*, vol. 12 2(2003): 287-326, pp. 298-299.

[333] Article 29 of the Explanatory Report of the Convention on Cybercrime.

admitted that 'the content of the communication' is sensitive,[334] they clarified that the definition and data preservation responsibility does not mean 'a revealing of the content of the communication'.[335] Rather, this definition and data preservation responsibility were just recommendations. National legislatures enjoy the ability to apply different definitions of 'traffic data' and reserve on the data preservation responsibility in their domestic law.[336]

However, these four key definitions are criticised by scholars as too broad to apply in judicial practice.[337] For instance, the definition of 'computer' does not limit what constitutes a device, thus may include cable TV boxes.[338] At the same time, such drawbacks are not the problem shared by the CoC itself.[339] Almost all the definitions raised by scholars are either too broad or too narrow. The issue of how to define computer, data, and others is still a hot topic even though several decades have already passed since their inception.

3.3.2 Offences against the security of computer

Offences under this category include illegal access, illegal interception, data interference, system interference and misuse of devices, namely, the ones threatening the confidentiality, integrity and availability of computer data and systems.

3.3.2.1 Illegal Access

Under Article 2, whoever intentionally secures access to the whole or any part of a computer system without right shall be punished. This offence is regarded as the 'basic offence'. It is the first step to conduct other dangerous acts, such as attacks against the security of computer system and computer trespass.[340]

Under this offence, mere hacking is criminalised since access to 'any part of a computer system' is included. On the one hand, according to the drafters of the CoC, such conduct may provide the possibility for the intruders to obtain confidential data (such as privacy) and secrets, and/or to obtain the use of a program without paying for it, and/or even encourage the

---

[334] *Ibid*.

[335] *Ibid*.

[336] Article 30 of the Explanatory Report of the Convention on Cybercrime.

[337] See e.g. Shannon L. Hopkins, 'Cybercrime Convention: A Positive Beginning to a Long Road Ahead', *Journal of High Technology Law*, vol. II 1(2003): 101-122.

[338] *Ibid*, p. 112.

[339] See e.g. Mike Keyser, 'The Council of Europe Convention on Cybercrime', *Journal of Transnational Law and Policy*, vol. 12 2(2003): 287-326.

[340] Article 44 of the Explanatory Report of the Convention on Cybercrime.

hackers to conduct more dangerous and harmful offences, such as computer-related fraud.[341] Therefore, the drafters of the CoC maintain that it 'should in principle be illegal in itself'.[342] Moreover, criminalising illegal access, the first step of further offences, can give additional protection to the system and the data and at an early stage.[343]

On the other hand, some scholars believed that criminalising mere hacking under the CoC was unnecessary. For instance, Indira Carr and Katherine S. Williams suggested that justifications of the offence illegal access provided in the ERCoC are based on 'economic grounds', which appear questionable.[344] To be specific, criminalising mere hacking was to prevent further and more severe offences, thus the time and monetary spent on investigating those crimes could be avoided, as well as the costs on security measures. However, they maintained that the costs of security measures and investigation could by no means be avoided, which makes it less necessary to leave mere hacking on the table in order to reduce such costs.[345] In addition, concerns about the possibility of over-criminalisation were raised on mere hacking.[346] The criminalisation of 'situations where no danger was created by the mere intrusion or where even acts of hacking have led to the detection of loopholes and weaknesses of the security of systems'[347] makes this provision itself controversial. Therefore, the offence of mere hacking became more difficult for the states to agree on.[348]

In this context, the signatories are granted considerable autonomy in criminalising this act with respect to the approach they take in their domestic laws. They can either take a broad approach or a narrow one, through attaching any or all of the qualifying elements to reduce the criminalisation of mere access, such as 'infringing security measures, and special intent to obtain computer data'.[349]

---

[341] *Ibid*.

[342] *Ibid*. For similar opinions see Lorenzo Picotti and Ivan Salvadori, 'National Legislation Implementing the Convention on Cybercrime –Comparative Analysis and Good Practices', *Strasbourg*: Council of Europe, 28 August 2008.

[343] Article 45 of the Explanatory Report of the Convention on Cybercrime.

[344] Indira Carr and Katherine S. Williams, 'Draft Cyber-Crime Convention: Criminalisation and the Council of Europe (Draft) Convention on Cyber-Crime', *Computer Law and Security Report*, vol. 18 2(2002): 82-90, p. 84.

[345] *Ibid*.

[346] David Banisar and Gus Hosein, 'A Draft Commentary on the Council of Europe Cybercrime Convention', Oct. 2002, available at http://readinglists.ucl.ac.uk/items/902E517A-C53D-6EA6-7B5F-D16577E06D64.html. Last visited May 2015.

[347] Article 49 of the Explanatory Report of the Convention on Cybercrime.

[348] *Ibid*.

[349] Article 50 of the Explanatory Report of the Convention on Cybercrime.

3.3.2.2 Illegal interception

Article 3, illegal interception, criminalises the unauthorised interception of non-public transmissions of computer data by technical means.[350] This provision aims to protect the confidentiality of computer data, the right to privacy in other words.[351] The reason of this offence is to maintain online-offline consistency. To be specific, traditional tapping and recording of oral telephone conversations between persons violates the privacy of communications, and thus it is an offence. Similarly, the interception conducted through a computer and a network also violates the privacy of communications, and should also be criminalised.[352] Therefore, the CoC introduces this offence, and applies it to all forms of electronic data transfer, including telephone, fax, email and file transfer.[353]

Apart from 'intentionally' and 'without right' as shared elements of cybercrime under the CoC, 'technical means' and 'non-public' are the other two qualifying elements. 'Technical means' refer to 'listening to, monitoring or the surveillance of the content of communications', [354] and 'non-public' 'qualifies the nature of the transmission (communication) process and not the nature of the data transmitted'.[355] In this sense, it does not matter where the communication takes place, either through a public network or private local networks, or even from the keyboard to the CPU.[356] It is non-public and protected by the CoC as long as the parties wish to keep it confidential.[357]

Considering that Article 3, as stated in the ERCoC, is drafted to protect the right to privacy,[358] it can be observed that through protecting computer data, the protection of the right to privacy can be enhanced. Despite the good attempt, the CoC leaves the issue of 'when the interception was legitimate' to domestic law to decide.[359] This actually leaves the issue of 'in which circumstances the information intercepted is private' to domestic law, as

[350] Article 3 of the Convention on Cybercrime, the Council of Europe.

[351] Article 51 of the Explanatory Report of the Convention on Cybercrime.

[352] *Ibid*.

[353] Article 51 of the Explanatory Report of the Convention on Cybercrime.

[354] Article 53 of the Explanatory Report of the Convention on Cybercrime.

[355] Article 54 of the Explanatory Report of the Convention on Cybercrime.

[356] *Ibid*.

[357] *Ibid*.

[358] Article 51 of the Explanatory Report of the Convention on Cybercrime.

[359] Article 58 of the Explanatory Report of the Convention on Cybercrime.

rightly pointed out by Prof. Carr.[360] It can be foreseeable that further explanation may be needed if the CoC intends to enhance the protection of the privacy.

3.3.2.3 Data interference

Article 4 protects computer data from intentional damage, deletion, deterioration, alteration or suppression without right.

Strictly speaking, this Article protects computer data away from being damaged. However, according to the ERCoC, this provision aims at protecting 'the integrity and the proper functioning or use of stored computer data or computer programs'.[361] Confusions with respect to the relationship between computer data and computer programs thus arise. On the one hand, the integrity of computer data is a virtual interest arising together with the development of information technology. On the other hand, a computer program is actually written and composed of computer data, and it is a product consists of computer data. In this regard, treating them as the same is like treating English and a book written in English as the same.

In addition, as indicated in the ERCoC, the 'integrity and the proper functioning' of a computer program is different from the integrity of computer data. The former focuses on the usage of a computer program, thus, it is the right of property that has long existed. However, the integrity of data is a virtual interest that did not exist before information technology. They are in essence different. It can thus be seen that the legal interests stated in the ERCoC are broader than the one protected by Article 4.

Moreover, the ERCoC mismatches the usage of a computer system and the integrity of computer data, and thus contradicts the approach reflected in the CoC. The CoC intends to distinguish between the integrity of computer data and the usage of a computer system. The two separate offences of data interference and system interference serve as an example of this intention. However, the ERCoC confused the integrity of data and the usage of a computer system. Firstly, although by definition a computer system is a device while a computer program is a set of instructions, the term 'computer program' is defined under the term 'computer system'.[362] This indicates that the 'computer program' is a hyponymy conception

[360] Indira Carr and Katherine S. Williams, 'Draft Cyber-Crime Convention: Criminalisation and the Council of Europe (Draft) Convention on Cyber-Crime', *Computer Law and Security Report*, vol. 18 2(2002): 82-90, p. 84.

[361] *Ibid*.

[362] Article 23 of the Explanatory Report of the Convention on Cybercrime.

of the 'computer system', and therefore not computer data. Secondly, the usage of a computer program focuses on its function, and makes it a property.[363] This treatment is as the same as the treatment of the computer system, i.e. being protected for the function.

3.3.2.4 System interference

Article 5 penalises the intentional hindering of the lawful use of computer systems.[364] It outlaws those acts referred to as computer sabotage in Recommendation No. R (89) 9, with the intention of protecting 'the interests of operators and users of a computer or telecommunication systems in being able to have them function properly'.[365] The term 'hindering' in Article 5 means 'actions that interfere with the proper functioning of the computer system'.[366]

Before convicting acts that hinder the function of a computer system, the hindering must be 'serious'. The criteria for deciding what damage is serious under the CoC contains, for instance, 'the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g. by means of programs that generate 'denial of service' attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system)'.[367] These criteria are not compulsory for the signatories; rather, they can enact their own standards, such as a minimum amount of damage to be caused.[368]

Spamming, which further developed into the DDoS attack in recent years, raises uncertainties of Article 5. Spamming is defined in the ERCoC as the action of sending out unsolicited email for commercial or other purposes and causing a nuisance to its recipients, in particular when such messages are sent in large quantities or with a high frequency.[369] From this definition one can notice that in the view of the drafters, only when the communications of

---

[363] 'Property' is defined as '1) the right to possess, use and enjoy a determinate thing; 2) any external thing over which the rights of possession, use, and enjoyment are exercised'. Item 'property' in Bryan A. Garner (ed.), *Black's Law Dictionary* (standard 9th edition), USA: West Publishing, 2009.

[364] *Ibid*.

[365] Article 65 of the Explanatory Report of the Convention on Cybercrime.

[366] Article 66 of the Explanatory Report of the Convention on Cybercrime.

[367] Article 67 of the Explanatory Report of the Convention on Cybercrime.

[368] *Ibid*.

[369] Article 69 of the Explanatory Report of the Convention on Cybercrime'.

computer systems are intentionally and seriously hindered, can the offender be criminalised.[370] Still, the signatories have the right to take a different standard to determine to what extent the function of a computer system should be interfered before such conduct can be considered as criminal.[371]

3.3.2.5 Misuse of devices

Article 6 establishes criminal liability for intentionally producing, selling or distributing 'access devices' that can be used to commit illegal acts that are listed under the CoC. The so-called 'access-devices', as explained in this Article, include computer programs, passwords, or similar data useful for committing any offence under the CoC.

This provision, according to the ERCoC, was drafted to combat the 'black market' that facilitated the sale or trade of the 'access devices'.[372] To conduct hacking offences, the offenders need to obtain means of access, i.e. 'access devices' under the CoC and 'hacker tools' under the ERCoC, or other tools. This necessity created a kind of black market selling or distributing these tools such as malware and Trojan horses.[373] Therefore, to better regulate cybercrime, the CoC prohibits the production, possession and distribution of programs or devices as they produce potential danger for further commissions.[374]

However, scholars hold different views on criminalising the 'access devices'. Some scholars challenged the necessity of this offence, especially on criminalising those dual-use devices. For instance, David Banisar and Gus Hosein argued that

> 'the focus should be on illegal conduct, not on the creation of tools that can be used for both legitimate and illegitimate purposes'.[375]

Other scholars, on the contrary, supported this offence by making an analogy between these 'access devices' and burglary tools. They maintained that many comprehensive criminal law systems regulating the physical world prohibit the tools used to commit crimes such as guns. Thus, by analogy, a proper and comprehensive criminal law regulating the virtual world

[370] *Ibid*.

[371] *Ibid*.

[372] Article 71 of the Explanatory Report of the Convention on Cybercrime.

[373] *Ibid*.

[374] *Ibid*.

[375] David Banisar and Gus Hosein, 'A Draft Commentary on the Council of Europe Cybercrime Convention', Oct. 2002.

should also prohibit the unauthorised production or distribution of criminal tools, in this case, the 'access devices'.[376]

Comparing these two sides, one can see that both of them acknowledged the threat and the danger presented by the 'access devices'. Their difference is whether the 'dual-use' devices should be prohibited. Thus, the essence of this issue becomes: many of the access devices are produced or distributed for testing purposes, is there a need to prohibit them?[377] To understand this issue and the purpose of Article 6, a closer scrutiny of the drafters' intention is helpful. Initially, the drafters limited the devices as 'those which are designed exclusively or specifically for committing offences' and thus excluding those dual-use devices. This definition, however, was found too narrow because 'it could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable, or only applicable in rare instances'.[378] In this context, an alternative way was to encompass a broad meaning that includes all devices no matter whether they were legally produced and distributed or not.[379] The drafters also rejected this way because it was too broad.[380] In the end, the drafters found a reasonable compromise: that 'only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment', with a restrictive supplement that the devices should be 'objectively designed, or adapted', and primarily for evil purposes.[381] Moreover, for the professionals need to use access tools to test the security of programs or systems, the drafters explained that only in a situation where the offender does not have the right of access, does he commit the offence of misuse of devices.[382] In this sense, if the professionals have the authority to test that program or system, he shall not be punished.

---

[376] Richard W. Downing, 'Shoring up the Weakest Link; What Lawmakers around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime', *Columbia Journal of Transnational Law*, vol. 43 (2005): 705-762, p. 733.

[377] Mike Keyser, 'The Council of Europe Convention on Cybercrime', *Journal of Transnational Law and Policy*, vol. 12 2(2003): 287-326, p. 304.

[378] Article 73 of the Explanatory Report of the Convention on Cybercrime.

[379] *Ibid*.

[380] *Ibid*.

[381] *Ibid*.

[382] Article 77 of the Explanatory Report of the Convention on Cybercrime.

3.3.3 Traditional crimes facilitated by computer

Offences proscribed under Articles 7-10 are traditional offences frequently committed through the use of a computer system, namely, computer facilitated forgery, fraud, child-pornography related offences, and copyright related infringements. The criminalisation of these offences indicates the illegal nature of the traditional offences committed through the use of computer system.[383] At the same time, however, it is not necessary for the signatories to criminalise these computer-facilitated offences as cybercrime. As Article 79 of the ERCoC states,

> 'most States already have criminalised these ordinary crimes, and their existing laws may or may not be sufficiently broad to extend to situations involving computer networks (for example, existing child pornography laws of some States may not extend to electronic images). Therefore, in the course of implementing these articles, States must examine their existing laws to determine whether they apply to situations in which computer systems or networks are involved. If existing offences already cover such conduct, there is no requirement to amend existing offences or enact new ones'.

According to this explanation, the reliance on traditional criminal law is the first choice of the signatories when criminalising wrongdoings facilitated by computer.[384] Drafting specific provisions serve as an additional option.

3.3.3.1 Computer-related offences

Article 7 of the CoC outlaws computer-related forgery, or, the unauthorised action that creates or alters electronically stored data and results in inauthentic data,[385] 'with fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another'.[386] It is

[383] Article 79 of the Explanatory Report of the Convention on Cybercrime.

[384] In the Convention, the offences under this category include computer-related fraud and forgery, offences related to child-pornography and offences related to infringements of copyright and related rights. The additional protocol to the Convention, i.e. the one came into force in 2006 and concerns the criminalisation of acts of a racist and xenophobic nature committed through computer systems, also establishes a subcategory of computer-related offences. This subcatogery is offences related to racist and xenophobic. Since this additional protocol takes the same approach of Art. 9 (offences related to child pornorgraphy) and Art. 10 (offences related to infringements of copytight and related rights), and the inclusion or not of this additional protocol will not lead to a different conclusion of this research, it was therefore left out from further and detailed discussion.

[385] Article 79 of the Explanatory Report of the Convention on Cybercrime.

[386] Article 90 of the Explanatory Report of the Convention on Cybercrime.

a parallel offence of forging tangible documents in the physical world,[387] to protect 'the security and reliability of electronic data which may have consequences for legal relations'.[388]

Clear as it may sound. However, the concepts of 'forgery' adopted by jurisdictions are developed from two perspectives.[389] Namely, some nations define it from the perspective of the author, and refer it to '[damage] the authentic as to the author of the document'; some others develop the concept from the perspective of the contents, and criminalise those acts '[damaging] the truthfulness of the statements contained in the document'.[390] After considering these two perspectives, the drafters of the CoC established a minimum standard of 'the deception as to authentic refers at minimum to the issuer of the data, regardless of the correctness or veracity of the contents of the data'.[391]

Article 8 of the CoC outlaws computer-related fraud. It rules that the intentional causing of loss of property by manipulating a computer system with dishonest intent is illegal. As the development of information technology, assets such as electronic funds, deposit money and credit cards becomes the criminals' target.[392] In this context, to prevent 'any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property',[393] the 'input', 'alteration', 'deletion' and 'suppression' of computer data, are outlawed under Article 8(a). Further, Article 8(b) supplements a general act of 'any interference with the functioning of a computer system' that causes a loss of property,[394] under which acts such as 'hardware manipulation', 'suppressing printouts' and 'affecting the recording or flow of data' is proscribed.[395]

[387] Article 81 of the Explanatory Report of the Convention on Cybercrime.

[388] *Ibid*.

[389] Article 82 of the Explanatory Report of the Convention on Cybercrime.

[390] *Ibid*.

[391] *Ibid*.

[392] Article 86 of the Explanatory Report of the Convention on Cybercrime.

[393] *Ibid*.

[394] Article 87 of the Explanatory Report of the Convention on Cybercrime.

[395] *Ibid.*

3.3.3.2 Offences related to child-pornography

Under Article 9, producing, offering, distributing, and transmitting child pornography are criminalised, as well as procuring and possessing relevant materials.[396] Article 9 is drafted to strengthen the protection for children against sexual exploitation, especially those committed through computer systems and networks.[397] Most jurisdictions have criminal provisions criminalising offences related to child-pornography. However, acts committed through computers and networks have different meanings compared with their traditional forms, according to the ERCoC. For instance, 'making available' under Article 9 covers 'the placing of pornography on line for the use of others, e.g. by means of creating child pornography websites',[398] and the 'possession' of child pornography means storing it on a computer system or a data carrier like a CD-room.[399] Therefore, modernising the traditional criminal provisions against child-pornography is necessary.

Under this Article, 'child-pornography' refers to

> 'pornographic material that visually depicts
>
> a) minor engaged in sexually explicit conduct;
>
> b) a person appearing to be a minor engaged in sexually explicit conduct;
>
> c) realistic images representing a minor engaged in sexually explicit conduct'.[400]

Moreover, it is not relevant whether the conduct prescribed under this Article is real or simulated,[401] and it is neither relevant whether the materials depicting such conduct are images of actual persons or are entirely generated by computers.[402]

3.3.3.3 Offences related to infringements of copyright and related rights

Article 10 criminalises the infringements of intellectual property which 'are among the most commonly committed offences on the internet, causing concern both to copyright holders and

[396] Article 93 of the Explanatory Report of the Convention on Cybercrime.

[397] Article 91 of the Explanatory Report of the Convention on Cybercrime.

[398] Article 95 of the Explanatory Report of the Convention on Cybercrime.

[399] Article 98 of the Explanatory Report of the Convention on Cybercrime.

[400] Article 9(2) of the Convention on Cybercrime, the Council of Europe.

[401] Article100 of the Explanatory Report of the Convention on Cybercrime.

[402] Article101 of the Explanatory Report of the Convention on Cybercrime.

those who work professionally with computer networks',[403] It protects works such as literary, photographic, musical, audio-visual and others.[404] In order to avoid over-criminalisation, Article 10 establishes two requisites of the offence under Article 10: the conduct must be committed on a 'commercial scale' and 'by mean of a computer system'.[405] In addition, unlike other offences prescribed in the Convention, the criminal liability is not pursued on the basis of 'intentionally'; rather, the infringements of copyright must be committed 'wilfully'. This change is to keep consistent with the term used in Trade-Related Aspects of Intellectual Property Rights ('TRIPS') Treaty, which governs 'the obligation to criminalise copyright violations'.[406]

3.3.4 Jurisdiction

Given the cross-border nature of cybercrimes, paragraph 1, Article 22 of the CoC attaches the territorial principle to offences under the CoC. The territorial principle, in the case of cyberspace, refers to a situation where a signatory has territorial jurisdiction if 'both the person attacking a computer system and the victim system are located within its territory, and where the computer system attacked is within its territory, even if the attacker is not'.[407] In addition, *litterae b* and *c* of paragraph 1, require signatories implementing a variant of the territorial principle over offences 'committed upon ships flying its flag or aircraft registered under its laws'.[408] Moreover, *litterae d* of paragraph 1, further establishes the nationality principle as a supplement. It requires the signatories having the ability to prosecute their own national if the conduct by this national is an offence under their domestic law, in case the state where the conduct took place does not have the ability to prosecute the offender.[409]

In conformity with their domestic laws, the signatories can declare reservation to *litterae b, c and d*,[410] they can also attach other types of criminal jurisdiction over cybercrimes.[411]

---

[403] Article107 of the Explanatory Report of the Convention on Cybercrime.

[404] *Ibid*.

[405] Lorenzo Picotti and Ivan Salvadori, 'National Legislation implementing the Convention on Cybercrime – Comparative Analysis and Good Practices', *Strasbourg*, Council of Europe, 28 August 2008, p. 38.

[406] Article 113 of the Explanatory Report of the Convention on Cybercrime. See also Mike Keyser, 'The Council of Europe Convention on Cybercrime', *Journal of Transnational Law and Policy*, vol. 12 2(2003): 287-326, p. 309.

[407] Article 233 of the Explanatory Report of the Convention on Cybercrime.

[408] Article 235 of the Explanatory Report of the Convention on Cybercrime.

[409] Article 236 of the Explanatory Report of the Convention on Cybercrime.

[410] Paragraph 2, Article 22 of the Convention on Cybercrime, the Council of Europe.

[411] Paragraph 4, Article 22 of the Convention on Cybercrime, the Council of Europe.

Considering the fact that one cyber attack may be launched in one state and the consequences happen in another, more than one party may have jurisdiction over this attack. On occasions like this, 'the affected parties can turn to consult each other in order to determine the proper venue for prosecution' in order to avoid duplication of effort,[412] but such consultancy is not obligatory.[413] This measure to address the jurisdiction conflicts seems practical. However, the CoC does not provide a mechanism to decide which of the affected countries has jurisdiction. In this situation, as Shannon L. Hopkins rightly points out, some criteria to decide the priority of jurisdiction would be helpful, which the CoC does not provide.[414]

3.4 Summary

Generally speaking, the CoC seeks to enhance the international harmonisation of domestic laws, so that similar behaviour is considered criminal internationally.[415] National laws on cybercrime, as suggested by Prof. Carr, 'have served national interests rather than guaranteeing or providing greater security for computer users'.[416] In this regard, a universally binding legal instrument will emphasise the advice of harmonising criminal laws to combat cybercrime.[417] Therefore, the CoC is drafted and has successfully attracted 48 ratifications and 6 signatories by April 2016.

Two distinctions serve as the characteristics of the CoC. They also indicate the legislative approach taken by the CoC. The first distinction is the one between the genuine cybercrime and the traditional crimes facilitated by computers. Considering the fact that there are several forms of cybercrime, some targeting computers or data stored on a computer and some are facilitated by computer or data, the drafters of the CoC distinguish 'offences against the confidentiality, integrity and availability of computer data and systems' and 'ordinary crimes that are frequently committed through the use of a computer system',[418] i.e. the genuine cybercrime and the traditional crime facilitated by computer. Through distinguishing these

[412] Article 239 of the Explanatory Report of the Convention on Cybercrime.

[413] Article 239 of the Explanatory Report of the Convention on Cybercrime.

[414] Shannon L. Hopkins, 'Cybercrime Convention: A Positive Beginning to a Long Road Ahead', *Journal of High Technology Law*, vol. II 1(2003): 101-122, p. 118.

[415] *Ibid*.

[416] Indira Carr and Katherine S. Williams, 'Draft Cyber-Crime Convention: Criminalisation and the Council of Europe (Draft) Convention on Cyber-Crime', *Computer Law and Security Report*, vol. 18 2(2002): 82-90, p. 88.

[417] *Ibid*, p. 88.

[418] Articles 18 and 79 of the Explanatory Report of the Convention on Cybercrime. See also Fausto Pocar, 'New Challenges for International Rules against Cybercrime', *European Journal on Criminal Policy and Research*, 10(2004): 27-37, p. 33.

two categories of cybercrime, the CoC harmonises criminal laws on the genuine cybercrime and at the same time provides a supplementary standard for traditional crimes facilitated by computer.

The second distinction is the one between the usability of a computer system and the integrity of computer data. As rightly pointed out by Richard W. Downing, an offender can damage the usability of a computer system and thus cause monetary loss, or harm the integrity or availability of information and thus make data unavailable.[419] In this sense, the CoC contributes to 'clarify these distinctions by addressing damage to data and damage to the functioning of computer systems in separate articles'.[420] For instance, Article 2 criminalises illegal access to computer, and Article 3 penalises illegal interception of computer data. This distinction, as some scholars have expressed, is a big step forward on systematically regulating cyberspace.[421]

However, the CoC fails to provide substantive criteria for determining what conduct is cybercrime. More importantly, there are inconsistencies between the legislative approach implied in the CoC and its Explanatory Report. For instance, Article 4 of the CoC protects computer data from being interfered, whereas Article 60 of the ERCoC treats computer data and computer program, a subordinate concept, the same.

With respect to the jurisdiction issue, some scholars expressed their concern that the territorial principle adopted in the CoC would 'appear to be of limited value' considering the transnational nature of cybercrime.[422] In this sense, the principle of nationality may be more suitable when cybercrimes are at issue, 'especially if it were to be used in relation to victims of cybercrime, since it would at least enable a state to protect its nationals, if not all the victims of the crimes'.[423]

---

[419] Richard W. Downing, 'Shoring up the Weakest Link; What Lawmakers around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime', *Columbia Journal of Transnational Law*, vol. 43 (2005): 705-762, pp. 726-728.

[420] *Ibid*, p. 728.

[421] See e.g. Global Internet Policy Initiative, 'Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime', September 2005, available at http://www.internetpolicy.net/cybercrime/20050900cybercrime.pdf. Last visited June 2015.

[422] Fausto Pocar, 'New Challenges for International Rules against Cybercrime', *European Journal on Criminal Policy and Research*, 10(2004): 27-37, p. 36.

[423] *Ibid*.

Chapter 4 The Cybercrime Legislation in the United States

4.1 Introduction

This Chapter intends to analyse the US legislation on cybercrime. 4.2 provides a wide range of background information on the cybercrime legislation through historical review, including the Computer and Fraud Abuse Act (hereafter the CFAA) 1984 and its eight Amendments in the decades following. 4.3 investigates and analyses the current legislation on cybercrime and the core contentious issues discussed in relation to cybercrime. Subsequently, 4.4 examines the scope of cybercrime in the US legal context and its attitude towards the Convention on Cybercrime. In the end, 4.5 summarises the characteristics of the cybercrime legislation in the US and the legislative approaches it takes against cybercrime. Noteworthy that the 'state' mentioned in this Chapter refers to the states that constitute the United States if not explained separately.

4.2 Historical Review of the Cybercrime Legislation in the US

The US has widely been known as one of the forerunners of attempting to use criminal law to regulate cyber wrongdoings, not only to use the then existing criminal law, but also to promulgate new laws. Such attempts can be traced back to the 1970s. Through historical review, 4.2 investigates how the legislation on cybercrime has developed, especially on the issue that how has the US struck the balance between online freedom and the control over cyberspace. Accordingly, 4.2 contains two parts: the first one is the evolution of the CFAA, and the second one is the competing considerations behind the CFAA in this evolving process.

4.2.1 The evolution of the Computer Fraud and Abuse Act

The first computer specific legislation in the US is the *Counterfeit Access Device and Computer Fraud and Abuse Act 1984*, which is changed into the *Computer Fraud and Abuse Act* in 1986. However, in the period from 1984 to 1986 there was no offence prosecuted under the CFAA 1984. The CFAA welcomed its first amendment in 1986. This Amendment introduces three new offences, reduces the *mens rea* requirement, and further defines several key terms in detail. Later, the 1988, 1989 and 1990 Amendments launch a 'campaign' to expand the scope of the CFAA. Following this campaign, the Amendment 1994 further reduces the *mens rea* requirement of several offences to 'recklessness', and the US National

Information Infrastructure Protection Act 1996 (hereafter the USNIIPA 1996) introduces criminal liability to negligent acts under certain circumstances. Soon after, the US Patriot Act of 2001 (hereafter the USPA 2001) broadens the jurisdiction over cybercrime cases to encompass 'computer[s] located outside of the United States', provided that computer was used to affect 'interstate or foreign commerce or communications of the United States'.[424]

After these amendments, the US signed the Convention on Cybercrime (hereafter the CoC) of the Council of Europe in 2001, and ratified it in 2006 after years of discussions on the advantages and disadvantages of ratifying and implementing it. The ratification of the CoC does not rein in the expanding tendency of the CFAA. In the years following, the US Identity Theft Enforcement and Restitution Act of 2008 (hereafter USITERA 2008) further adds that if a computer 'is used in or affecting interstate or foreign commerce or communication…', it is a 'protected computer' and the US has jurisdiction over it.[425]

Table 4.1 the eight Amendments to the CFAA in the history

Title	Main amendments
The Amendment 1986	a. Affirms that 'exceed authorisation' is different from 'without authorisation'; b. substitutes 'intentionally' for 'knowingly'.
The Amendment 1988	Broadens the scope of 'financial institution' that it no longer limits to the ones issuing credit cards.
The Amendment 1989	'Bank' is added as 'financial institution'.
The Amendment 1990	Two more subparagraphs are added under 'financial institution' as (H) and (I).
the Amendment 1994	Affirms under certain occasions 'adverseness' and 'recklessness' shall be criminalised.
The National Information Infrastructure Protection Act 1996	a. Information of 'financial institutions' is replaced by in fact any information of any computer used for interstate or foreign commerce or communication; b. Computer extortion is criminalised; c. 'A threat to public health or safety' is added as a kind of damage the actor of computer misuse caused;

[424] 18 U.S.C. § 1030(e)(2)(B). Before this amendment, the 'protected computer' was defined to include 'one of two or more computers used in committing the offence, not all of which are located in the same State'.

[425] 18 U.S.C. § 1030(e)(2)(B). This part was originally worded as 'is used in interstate or foreign commerce or communication'.

	d. 'Financial interests' computer is added as 'protected computer'.
The Patriot Act 2001	Broadens the scope of 'protected computer'.
The Identity Theft Enforcement and Restriction Act 2008	a. Inserts a subparagraph 'affects ten or more protected computer during any 1-year period' as a kind of harm; b. Further broadens the scope of 'protected computer'.

With the CFAA 1984 and its eight Amendments, the current cybercrime legislation in the US has been established.[426] According to the promulgation of the CFAA and its Amendments, the four decades of the US' efforts can be divided into three periods: (1) pre 1984 – initial efforts in drafting a cybercrime legislation, (2) from 1984 to 1986 – the first piece of legislation focusing on cybercrime, and (3) from 1986 to 2008 – expansions and amendments.

4.2.1.1 Pre 1984: initial efforts in drafting a cybercrime legislation

Regarding cybercrime as a dangerous consequence of introducing computers to American society, the US enacted the Counterfeit Access Device and Computer Fraud and Abuse Act, more commonly referred to as the Computer Fraud and Abuse Act (it can also be referred to as 18 U.S.C. § 1030) in 1984. Before this Act, the efforts of using criminal law to regulate cyber wrongdoing had been traced back to the 1970s. Namely, the efforts on the first US Bill of the Federal Computer Systems Protection Act (hereafter the BFCSPA) of 1977.

Some legal experts maintained that computer crimes were nothing but traditional crimes committed by new technological devices, and they could be tackled by traditional criminal theories.[427] Therefore, they attempted applying traditional criminal provisions on cyber wrongdoings. To be specific, in the Federal Criminal Code, there were many different laws under Title 18 that could possibly apply to cybercrime.[428] They were, for instance, laws on theft and related offences (e.g. 18 U.S.C. § 641, embezzlement or theft of public money,

[426] See e.g. Greg Pollaro, 'Display Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope', *Duke Law and Technology Review,* 12 (2010): i. See also Orin S. Kerr, 'Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes', *New York University Law Review,* vol. 78 5(2003): 1596-1668.

[427] See e.g. Michael Gemignani, 'Computer Crime: The Law in "80"', *Indiana Law Review*, vol. 13 (1980): 681- 723. See also Donald G. Ingraham, 'On Charging Computer Crime', *Computer/Law Journal*, vol. 2 (1980): 429-439.

[428] Susan Hubbell Nycum, 'The Criminal Law Aspect of Computer Abuse: Part II Federal Criminal Code', *Journal of Comptuers and Law*, vol. 5 (1975): 297-322.

property or records), abuse of Federal Channels of Communication (e.g. 18 U.S.C. § 1341, mail fraud), national security offences (e.g. 18 U.S.C. § 793, gathering, transmitting, or losing defence information), trespass and burglary (e.g. 18 U.S.C. § 2152, trespass on fortifications or harbour defence areas), deceptive practice (e.g. 18 U.S.C. § 912, obtaining thing of value by impersonating an officer or employee of the United States) and property destruction (e.g. 18 U.S.C. § 81, arson within special maritime and territorial jurisdiction).

Other scholars contested that the reliance on traditional theories could not help combat cybercrime, and new laws and enforcement measures were required to address them.[429] For instance, Susan Nycum pointed out that the abovementioned statutes merely 'may be applicable to computer abuse'.[430] Since none of them was drafted with an eye on the involvement of computers in crimes,[431] each of them had defects when combating computer crimes. For instance, in the case *United States v. Seidlitz*[432] the defendant would not have been convicted if he had not committed the crime across state borders.[433] In other words, the provisions against wire fraud could not be applied to computer fraud, unless the computer fraud was committed cross state border. The element of 'cross state border' was not as common as it is today. Therefore, it was this accidental factor that made the act a criminal offence.

Starting from this case, scholars gradually realised that the then existing statutes did not and could not perform effectively in cases involving computers. Further, they gradually realised

---

[429] See e.g. Rob Kling, 'Computer Abuse and Computer Crime as Organizational Activities', *Computer/Law Journal*, vol. 2 (1980): 403-427.

[430] Susan Hubbel Nycum, 'The Criminal Law Aspects of Computer Abuse – Part II: Federal Criminal Code', *Journal of Computers and Law,* 5(1976): 297-322, p. 297. Similar to Nycum's opinion, the Congressional Record of the 96th Congress also stated that since these laws were not drafted with the intention to encompass crimes committed through technical means and devices, federal prosecutors found themselves 'handicapped' in constructing their cases on proper provisions. Congressional Record, S. 240, 96th Cong., 1st Sess., 125 Cong. Rec. 710 (1979).

[431] Congressional Record, S. 240, 96th Cong., 1st Sess., 125 Cong. Rec. 710 (1979).

[432] *United States v. Seidlitz*, 589 F.2d 152 (4th Cir. 1978). In this case, Seizlitz gained access to the computer system of Optimum Systems, Inc. (hereafter OSI) that he used to work for by telephone the OSI facility from another state. He was charged under 18 U.S.C. § 1343, with wire fraud, on the factual basis that he transmitted two telephone calls in interstate commerce of a scheme to defraud OSI of property consisting of information from the computer system. 18 U.S.C. § 1343 prohibited explicitly transmission by wire communication of any writings, signs, signals, pictures or sounds for the purpose of executing a scheme to defraud or to obtain money or property by means of false or fraudulent pretences or representations. A conviction was obtained by district court of fraud by wire and was maintained in appellate court. For detailed information about this case, see http://law.justia.com/cases/federal/appellate-courts/F2/589/152/193998/. Last visited March 2015.

[433] *United States v. Seidlitz*, 589 F.2d 152 (4th Cir. 1978). See also John Roddy, 'The Federal Computer Systems Protection Act', *Journal of Computers, Technology and Law,* 7(1976): 343-365, p. 344. Situations as such also appeared in *United States v. Lester* (under 18 U.S.C. § 2314), *United States v. Astolas* (under 18 U.S.C. § 659), and others.

that wrongdoings targeting or facilitated by computers were 'inherently different' from wrongdoings accomplished by other means, so crimes with a computer feature were a new and unique category of criminal conduct.[434] In this context, the legislators realised that the traditional laws could provide little chance of criminalising cyber wrongdoings, and the prosecutors and judges tried hard to bring the accused's act under the traditional law.[435]

Against this background, the consensus for a technology-specific statute was reached. As a response to this consensus, legislators drafted the BFCSPA to solve the issue of lacking specific legislation.[436] Under this Bill, 'the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce…' were criminalised.[437] To be specific, it outlawed

> 'any knowing and wilful manipulation, or attempted manipulation, of a "computer, computer system, computer network, or any part thereof…: 1) devising or executing any scheme or artifice to defraud, or 2) obtaining money, property, or services, for themselves or another, by means of false or fraudulent pretences, representations, or promises…"'.[438]

In addition, any impairment of computer, computer system, computer data or computer network was also criminalised under the BFCSPA. Put it in detail, the BFCSPA also criminalised intentionally and without authorisation, directly or indirectly accessing, altering, damaging, destroying or attempting to damage or destroy any computer, computer system, or computer network, or any computer software program or data contained in mentioned devices.[439]

Criminalising almost all the unauthorised accesses, the BFCSPA categorised these acts into four types, including

---

[434] Joseph M. Olivenbaum, '<Ctrl> <Alt> <Del>: Rethinking Federal Computer Crime Legislation', *Seton Hall Law Review,* vol. 27 (1997): 574-641, pp. 590-591.

[435] In the 1984 House Judiciary Committee Report the Department of Justice also admitted that 'there would have been no basis for Federal prosecution' if the defendant did not gain access to the targeted computer system through interstate telephone lines. See Joseph M. Olivenbaum, '<Ctrl> <Alt> <Del>: Rethinking Federal Computer Crime Legislation', *Seton Hall Law Review,* vol. 27 (1997): 574-641, pp. 591-592.

[436] John Roddy, 'The Federal Computer Systems Protection Act', *Journal of Computers, Technology and Law,* 7(1976): 343-365, pp. 344-350.

[437] Congressional Record, S. 240, 96th Cong. 1st Sess., § 1028(a) (1979).

[438] Congressional Record, S. 240, 96th Cong. 1st Sess., §1028(a)(2) (1979).

[439] See John Roddy, 'The Federal Computer Systems Protection Act', *Journal of Computers, Technology and Law,* 7(1976): 343-365, p. 350.

> 'the introduction of fraudulent records or data into the computer systems;
>
> the unauthorised use of computer related facilities;
>
> the alteration or destruction of information or files; and
>
> the stealing, whether by electronic means or otherwise, of money, financial instruments, property, services, or valuable data.'[440]

Analysing from the outlawed behaviour and the categories of the BFCSPA, one can see that its intended criminalising scope was broad, including securing access to computers without authorisation, altering data to computer systems, and even stealing money. Admittedly, in a stage that nobody understood the nature of cybercrime, such a broad scope could serve to regulate cyber wrongdoing at the same time avoid precisely defining it. However, the criminalisation scope of the BFCSPA was 'extremely broad', therefore potentially penalised a large part of computer professional practices, as commented by scholars.[441] In addition, the definition of 'computer' under the BFCSPA was also criticised as too broad: it encompassed not only computer in a common sense but also pocket calculators and digital watches.[442] More importantly, this Bill presented a serious threat to privacy by abusing the powers granted to law enforcement agencies, because 'any computer in America [would] be accessible for the first time to investigation by a major Federal law enforcement agency'.[443]

Considering these criticisms, legislators did not pass the BFCSPA. Moreover, the final published CFAA was intentionally restricted, both in the criminalising scope and the enforcement measures granted to agencies, in order to avoid redundancy and over-reaching.[444]

---

[440] Congressional Record, S. 240, 96th Cong., 1st Sess., 125 Cong. Rec. 710 (1979).

[441] For instance, some security measures taken by programmers may face criminal charge. See John K. Taber, 'On Computer Crime (Senate Bill S. 240)', *Computer/Law Journal,* 1(1978-1979): 517-543, pp. 530-532.

[442] John K. Taber, 'On Computer Crime (Senate Bill S. 240)', *Computer/Law Journal,* 1(1978-1979): 517-543, p. 532. See also John Roddy, 'The Federal Computer Systems Protection Act', *Journal of Computers, Technology and Law,* 7(1976): 343-365, pp. 357-361. Nycum argued in this article that the definitions in bills such as the BFCSPA, should be 'carefully worded so as to be broad enough to include non-electronic computers which [were] presently excluded from the legislation's scope; narrow enough to exclude a variety of electronic devices which rely on micro-processing circuitry which may be included; and flexible enough to cover technological advances'.

[443] John K. Taber, 'On Computer Crime (Senate Bill S. 240)', *Computer/Law Journal,* 1(1978-1979): 517-543, pp. 532-536. Senator Biden expressed his opinion at the hearings on S. 240 that this Bill meant that 'just about any computer in America will be accessible for the first time to investigation by a major Federal law enforcement agency'.

[444] Jo-Ann M. Adams, 'Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet', *Computer and High Technology Law,* 12 (1996): 403-434, p. 421.

4.2.1.2 From 1984 to 1986: the first legislation focusing on cybercrime

The CFAA passed in 1984 was the first federal law specifically against cybercrime. It introduced three offences: '(1) accessing a computer to get classified defence or foreign relations information to harm the United States or to advantage a foreign nation, (2) accessing a computer to get financial records from a financial institution or consumer information from consumer reporting agencies, and (3) modifying, destroying, or disclosing information if such conduct affects the government's use of the computer',[445] and covers situations 'when the crime was interstate, when harm was done to financial institution computers, or when the crime was perpetrated against the federal government's own computers'.[446]

However, the CFAA 1984 was in fact not applicable or sufficient in practice, supported by the fact that there had been no prosecution under the CFAA 1984 since its promulgation in the next two years.[447] Firstly, as mentioned above, the CFAA 1984 was drafted with the intention to limit its scope and avoid infringement of individual privacy and freedom. Bearing this in mind, the CFAA only introduced three offences, and merely provided protection for national security secrets, financial records and consumer information, and government property, all of which concerned government or economic interests. Therefore, the computers belonging to individuals or not relating to financial records or consumer information were out of its reach. Accordingly, personal information stored on personal computers, or not on personal computers but not relating to financial records such as credit cards, was neither protected under the CFAA.[448] Secondly, the 'knowledge' requirement for a conviction was higher than the constituent elements required in other relevant statutes.[449] For instance, Dodd S. Griffith pointed out that § 1030(a)(1) required the defendant 'knew the protected information was to be used to harm the United States or to help a foreign nation'; nonetheless, other relevant provisions only required that the defendant 'had a reason to believe that the information could be used to harm the United States or to the advantage of a foreign

[445] 18 U.S.C. § 1030(a)(1)-(3).

[446] Brandon Darden, 'Definitional Vagueness in the CFAA: Will Cyber-bullying Cause the Supreme Court to Intervene?' *Southern Methodist University Science and Technology Law Review*, vol. XIII (2010): 329-358, p. 331.

[447] Jo-Ann M. Adams, 'Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet', *Computer and High Technology Law Journal,* 12(1996): 403-434, p. 422.

[448] *Ibid*.

[449] See e.g. Dodd S. Griffith, Note, 'The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem', *Vanderbilt Law Review,* vol. 43 2(1990): 453-490.

country'.[450] Thirdly, one inconsistency existed in the CFAA, that if a person gained access to a computer with authorisation, and then he obtained the information to which he was not authorised; there would be no charge for obtaining and using such information.[451] In other words, the CFAA 1984 could not deal with situations where the actor exceeded his authorisation. As being criticised, the existence of such a situation was clearly not in line with the Congressional intention for the CFAA 1984.[452]

4.2.1.3 After 1986: expansions and amendments

(1) The 1986 Amendment: make the CFAA applicable

Considering the inapplicability or insufficiency of the CFAA 1984, an Amendment (hereafter Amendment1986) was made two years later. This Amendment expanded the reach of this statute and made it applicable in practice.[453] The changes made by this Amendment are as follows.

Firstly, as a response to the criticism shared by the Department of Justice and scholars, the Amendment 1986 replaced the intent element from 'knowingly' to 'intentionally' for offences under 18 U.S.C. § 1030 (a)(2) and (a)(3), and expanded the *actus reus* so as to include exceeding authority. Under the CFAA 1984, the *actus reas* element was prescribed as 'having accessed a computer without authorisation'.[454] The Amendment 1986 rephrased this wording and inserted 'exceeds authorised access', which was further explained as 'to access a computer with authorisation and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter'.[455]

Secondly, the Amendment 1986 introduced three new offences: (1) prohibiting accessing without right with intent to defraud, i.e. subsection 18 U.S.C. § 1030 (a)(4); (2) altering, damaging or destroying the information after unauthorised access or preventing authorised use, i.e. subsection 18 U.S.C. § 1030 (a)(5); and (3) trafficking in computer passwords, i.e. subsection 18 U.S.C. § 1030 (a)(6).

---

[450] *Ibid*, p. 467.

[451] Jo-Ann M. Adams, 'Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet', *Computer and High Technology Law Journal,* 12(1996): 403-434.

[452] *Ibid*, p. 422.

[453] Orin S. Kerr, 'Vagueness Challenges to the Computer Fraud and Abuse Act', *Minnesota Law Review,* vol. 94 (2009): 1561-1587, p. 1564.

[454] 18 U.S.C. § 1030(a)(1) (1984).

[455] 18 U.S.C. § 1030(e)(6) (1986).

Thirdly, the CFAA inserted paragraph (B) under the original definition of 'federal interest computer', thus expanded the scope of this term. Among these newly introduced three offences, offences under subsections (a)(4) and (a)(5) were limited to those affecting 'federal interest' computers.[456] As defined in the CFAA, the 'federal interest' computers were computers that are

> '(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 offences affecting that use of the financial institution's operation or the Government's operation of such computer; or
>
> (B) which is one of two or more computers used in committing the offences, not all of which are located in the same State'.[457]

Paragraph (A) almost shared the same coverage as the one in the CFAA 1984, while the ground supplemented under paragraph (B) stretched the reach of 'federal interest computer'. For the most part, the new ground set by paragraph (B) was for crimes where state law enforcement agencies lacked jurisdiction. However, this new ground was still criticised as 'quite limited',[458] because the Senate Judiciary Committee intended the jurisdiction over computer crimes at the federal level must be based on the 'interstate element', as suggested in the Senate Report No. 99-432 (1986).[459] Also in this report, computer crimes with 'interstate element' were explained as offences involving a 'compelling federal interest' or where 'the crime itself is interstate in nature'.[460]

(2) The 1988, 1989 and 1990 Act – efforts to enhance financial security

In the later years, three more Amendments were made to the CFAA in 1988, 1989 and 1990 respectively. Theses three Amendments further expanded the scope of the CFAA. The Amendment 1988 broadened the wording 'financial institutions' in subsection (a)(2) to cover

---

[456] 18 U.S.C. § 1030(a)(4)-(5) (1986).

[457] 18 U.S.C. § 1030(e)(2) (1986).

[458] See e.g. Orin S. Kerr, 'Vagueness Challenges to the Computer Fraud and Abuse Act', *Minnesota Law Review*, vol. 94 (2009): 1561-1587.

[459] Cited in Orin S. Kerr, 'Vagueness Challenges to the Computer Fraud and Abuse Act', *Minnesota Law Review*, vol. 94 (2009): 1561-1587. This Report explained the Senate Judiciary Committee's objective to limit federal jurisdiction over computer crimes by adding 'interstate elements'.

[460] *Ibid.*

all financial institutions rather than those issuing credit cards only. In the Amendment 1989, 'a bank' was replaced with 'an institution' in subsection (e)(4)(a), and stated explicitly that 'an institution with accounts insured by the Federal Savings and Loan Insurance Corporation' was included. As the result of these changes, 'any institutions with deposits insured by the FDIC (i.e. Federal Deposit Insurance Cooperation)' were included.[461]

In the Amendment 1990, two more types of financial institutions were added into subsection (e)(4), expanding the scope of 'financial institutions' further:

> '(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
>
> (I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act'.[462]

(3) The Amendment 1994 – the expansion to reckless act

The Amendment 1994 mainly expanded the *mens rea* of the offence under 18 U.S.C. § 1030(a)(5) to include 'recklessness'. 18 U.S.C. § 1030(a)(5) is widely known as the 'virus statute',[463] and it aims to regulate the unauthorised transmission of a program, information, code or command, namely, computer virus. Before the 1994 Amendment, the offence under 18 U.S.C. § 1030(a)(5) was phrased as 'knowingly altering, damaging, or destroying data, or preventing authorised use of the computer'. After the Amendment 1994, this offence covered two grounds: paragraph (A) penalises acts that intentionally cause damage, and paragraph (B) criminalises intentional access which recklessly causing damage.[464]

(4) The National Information Infrastructure Protection Act of 1996 – the broader, the 'better'

---

[461] Jo-Ann M. Adams, 'Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet', *Computer and High Technology Law Journal,* 12(1996): 403-434, pp. 424-425.

[462] 18 U.S.C. § 1030(e)(4) (1990).

[463] Joseph M. Olivenbaum, '<Ctrl> <Alt> <Del>: Rethinking Federal Computer Crime Legislation', *Seton Hall Law Review,* vol. 27 (1997): 574-641, p. 586.

[464] 18 U.S.C. § 1030(a)(5) (1994).

'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; or (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage'

shall be punished.

In the line of expansion, the NIIPA 1996 broadened the scope of the original statute mainly in four ways.

First of all, the subject of the offence under subsection (a)(2) is expanded. Initially, only the computers used by financial institutions, card issuers, or consumer-reporting agencies were protected. After being changed in 1996, any information of any kind stored on any computer is protected, only if an interstate or foreign element is involved in this conduct.[465] To be clearer, initially, only obtaining information contained on a financial record of a financial institution or in a file of a consumer reporting agency on a consumer was criminalised;[466] and after 1996 any obtaining of information shall be punished, as long as the computers involved locate in more than one states.

Not surprisingly, this change provoked concern about over-criminalisation. For instance, someone had pointed out that the wording of 'obtaining information' might include merely reading it.[467] Reading this understanding together with the change regarding the enlarged scope of protected information, merely reading or viewing any information of any kind shall be punished, as long as such reading was done through interstate or foreign communication.[468] Other scholars were not much concerned of the possibility of over-criminalisation. They developed their argumentation on the basis of court's interpretation of 'obtaining information'. That is, 'obtaining anything of value' required 'more than simply viewing information, such as printing, recording, or using the information', as the case *United States v. Czubinski*[469] shows.[470]

---

[465] 18 U.S.C. § 1030(a)(2)(C) (1996).

[466] 18 U.S.C. § 1030(a)(2) (1986).

[467] See S. Rep. No. 99-432 (1986) (emphasising that 'obtaining information' used in this statute includes 'mere observation of the data').

[468] See e.g. Orin S. Kerr, 'Vagueness Challenges to the Computer Fraud and Abuse Act', *Minnesota Law Review,* vol. 94 (2009): 1561-1587, pp. 1566-1567.

[469] *United States v. Czubinski,* 106 F.3d 1069 (1st Cir. 1997). In 1992, Czubinski carried out numerous unauthorised searches of the Integrated Data Retrieval System (IDRS) files. He knowingly disregarded the Internal Revenue Service (IRS) rules by looking at confidential information obtained by performing computer searches that were outside of the scope of his duties as a Contact Representative. For example, Czubinski accessed information regarding: the tax returns of two individuals involved in the David Duke presidential campaign; the joint tax return of an assistant district attorney and his wife; the tax return of Boston City Counselor Jim Kelly's Campaign Committee; the tax return of one of his brothers' instructors. Czubinski also accessed the files of various other social acquaintances by performing unauthorised searches. Nothing in the record indicates that Czubinski did anything more than knowingly disregard IRS rules by observing the confidential information he accessed. No evidence suggests, nor does the government contend, that Czubinski disclosed the confidential information he accessed to any third parties. The government's only evidence demonstrating any intent to use the confidential information for nefarious ends was the trial testimony of William A. Murray. Murray testified that Czubinski had once stated at a social gathering that 'he intended to use some of that information to build dossiers on people' involved in 'the white supremacist movement.' There is,

Secondly, a new offence was inserted as 18 U.S.C. § 1030(a)(7), which penalises computer extortion. This issue is discussed in 4.3 of this Chapter, the current legislation on cybercrime, in detail.

Thirdly, by expanding the list of damage to computers prescribed in § 1030(c)(4)(A)(i), the range of computer damage was enlarged. Two new forms of damages are added, including 'physical injury to any person'[471] and 'a threat to public health or safety'.[472]

Finally, the term 'federal interest computer' was replaced by a new term: 'protected computer'. Defined by the NIIPA 1996, a 'protected computer' refers to a computer that is:

> '(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 offences affects that use by or for the financial institution or the Government; or
>
> (B) which is used in interstate or foreign commerce or communication'.[473]

Compared with the definition of 'federal interest computer', the main change was in paragraph (B). It was changed from 'one of two or more computers used in committing the offences, not all of which are located in the same State' to this new phrasing. 'Federal interest computer', as phrased in the original definition, were computers located in more than one states. However, the 'protected computers' merely require a computer used in interstate commerce or communication. This replacement, as criticised by legal scholars, expanded the scope of this definition significantly.[474] For instance, Orin Kerr, a legal professor, pointed out that every computer connected to the Internet was arguably used in interstate commerce

---

however, no evidence that Czubinski created dossiers, took steps toward making dossiers (such as by printing out or recording the information he browsed), or shared any of the information he accessed in the years following the single comment to Murray. The record shows that Czubinski did not perform any unauthorised searches after 1992.

He was convicted on nine counts of federal wire fraud under 18 U.S.C. § 1343 and 1346, and four counts of federal interest computer fraud under 18 U.S.C. § 1030(a)(4). His conviction was reversed in the appeal on all counts.

[470] See e.g. Michael Hatcher, Jay McDannell and Stacy Ostfeld, 'Computer Crimes', *American Criminal Law Review,* vol. 36 (1999): 397-444, p. 407.

[471] 18 U.S.C. § 1030(c)(4)(A)(i)(III) (1996).

[472] 18 U.S.C. § 1030(c)(4)(A)(i)(IV) (1996).

[473] 18 U.S.C. § 1030(e)(2) (1996).

[474] See e.g. Orin S. Kerr, 'Vagueness Challenges to the Computer Fraud and Abuse Act', *Minnesota Law Review,* vol. 94 (2009): 1561-1587.

and communication, because the Internet *per se* was an interstate network that used for commerce and communication.[475] If this interpretation holds true, every computer connected to the Internet is a 'protected computer' for the purpose of the NIIPA 1996, and therefore, every conduct targeting any computer connected to the Internet would be punished.

(5) The Patriot Act 2001 – the expansion of 'protected computer'

The US Patriot Act 2001 (hereafter the PA 2001) further expands the scope of 'protected computers'. To be specific, it replaces paragraph (B) of 'protected computers' with any computer 'which is used in interstate or foreign commerce or communication, including a computer located outside the US that is used in a manner that affects interstate or foreign commerce or communication of the United States'.[476] Thus, the concern of any computer was a 'protected computer' after the NIIPA 1996 came true. This replacement, as expressed by the Computer Crime and Intellectual Property Section Criminal Division, clearly showed that 'protected computer' includes computers outside of the US only if the requirement of 'interstate or foreign commerce or communication' was satisfied.[477]

(6) The Identity Theft Enforcement and Restitution Act 2008 – a follower of expansion

As the same as the previously introduced Amendments, the US Identity Theft Enforcement and Restitution Act 2008 (hereafter the ITERA 2008) also follows the trend of expansion, and makes three notable changes to the CFAA. First of all, it deletes the requirement of 'interstate or foreign commerce or communication' from § 1030(a)(2). According to the newest version of this subsection, 'any unauthorised access to any protected computer that retrieves any information of any kind, interstate or intrastate, is punishable by the statute'.[478]

Secondly, the ITERA 2008 expands the list of damages to computers. It inserts that if the damage affects 'ten or more protected computers during any 1-year period', it is an offence under § 1030(c)(4)(A).

Thirdly, the ITERA 2008, again, expands the scope of 'protected computers' to an enormous degree. The present definition of 'protected computers' is the computers that

---

[475] *Ibid*, pp. 1567-1568.

[476] 18 U.S.C. § 1030(e)(2) (2001).

[477] *Prosecuting Computer Crimes*, Computer Crime and Intellectual Property Section Criminal Division, Published by Office of Legal Education Executive Office for United States Attorneys, 2010, p. 5.

[478] 18 U.S.C. § 1030(a)(2)(C) (2008). See Orin S. Kerr, 'Vagueness Challenges to the Computer Fraud and Abuse Act', *Minnesota Law Review,* vol. 94 (2009): 1561-1587, p. 1569.

> '(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 offences affects that use by or for the financial institution or 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'.[479]

Consequently, the 'protected computers' covers computers that used in or affecting interstate commerce or communication in judicial practice, inside or outside of the US.[480] This definition and its interpretation, as maintained by legal scholars, indicate a signal of the intent of the Congress to cover and regulate as many computers as being allowed.[481]

Generally speaking, after the CFAA 1984 and its eight Amendments, the current cybercrime legislation in the US is established. Although the legislators intentionally restricted the reach of the CFAA when drafting it, the amendments expanded its scope to an enormous degree. All of the changes made by the Amendments were either introducing new offences or expanding the coverage of the terms. In this process, even though legal scholars expressed their concern over the possibility of over-criminalisation, the continuous confirmations on the expansions from the legislature pale the concern.

4.2.2 Competing arguments behind the legislation

While several groups maintained that the traditional criminal laws applied to computer crime and thus there was no need for new legislation, some others argued that the need for a specific legislation on computer crimes could not be ignored. This discussion started in the 1970s and lasts till today. In this discussion, not only the civil liberties and national security,

---

[479] 18 U.S.C. § 1030(e)(2) (2008).

[480] See e.g. *United States v. Drew*, 259 F.R.D. 449, 457 (C.D. Cal. 2009) and *United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007). In both cases the courts held that it is enough for jurisdiction that a computer connects to the Internet. The proof that the defendant used the Internet to access the computer or use the computer to access the Internet is not required. See *Prosecuting Computer Crimes*, Computer Crime and Intellectual Property Section Criminal Division, Published by Office of Legal Education Executive Office for United States Attorneys, 2010, pp. 4-5.

[481] See e.g. Orin S. Kerr, 'Vagueness Challenges to the Computer Fraud and Abuse Act', *Minnesota Law Review,* vol. 94 (2009): 1561-1587, p. 1570.

but also the deterrence of a criminal offence and the uniformity of states' reaction to computer crimes are involved.

4.2.2.1 Arguments against a cyber-specific legislation

The arguments against specific legislation on computer crimes can be summarised as the following.

Firstly, the information technology has been developed and will continue to develop at a speed that the legislation cannot match. If there were a specific legislation regulating every change presented by the development in technology, the Congress would always face the issue of whether to amend the legislation so as to reflect every single change. The law enforcement agencies would also face the issue of how to interpret new legislation. In this regard, the best way for the Congress as well as for the law enforcement agencies is to rely on the existing laws.[482]

The second reason for no cyber-specific legislation is regarding the possibility of abusing powers, and thus the possibility of infringing civil liberties and over-criminalisation.[483] For the case of civil liberties, new offences will be inevitably escorted by new investigative powers of law enforcement agencies, and the new powers may be abused. For instance, the new investigative power creates a threat to the confidentiality of information. Take personal information stored on computers as an example. The right to privacy has long been established in *Griswold v. Connecticut* in 1965. When hearing this case, the Supreme Court recognised the right to privacy was a fundamental and constitutional right, implicitly documented in the Bill of Rights.[484] As technology develops, the record-keeping function of digital devices is gaining in popularity. Not only the computers, but also the mobile phones and others are equipped with record-keeping function. In this regard, if the law enforcement agencies have legal access to the information stored on computers and other digital devices, they may abuse this power.[485] As Senator Biden puts it:

---

[482] See Jo-Ann M. Adams, 'Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet', *Computer and High Technology Law Journal,* 12(1996): 403-434.

[483] See e.g. John K. Taber, 'On Computer Crime (Senate Bill S. 240)', *Computer/Law Journal*, 1(1978-1979): 517-543, pp. 532-533. The civil liberty groups and organisations include, for instance, the American Civil Liberties Union, the Electronic Privacy Information Centre and Privacy International.

[484] See Griswold v. Connecticut, 381 U.S. 479 (1965), available at https://supreme.justia.com/cases/federal/us/381/479/case.html. Last visited March 2015.

[485] See e.g. Charlotte Decker, 'Notes, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime', *Southern California Law Review,* vol. 81(2008): 959-1016, p. 1003.

> 'We are going to be turning to these agencies and saying "We are going to broaden your jurisdiction now. We are going to allow you legally to get into a number of data banks that you did not have access before."…Your legislation is very broad. As I read it, just about any computer in American will be accessible for the first time to investigation by a major Federal law enforcement agency.'[486]

For the case of over-criminalisation, the abuse of investigating and prosecuting powers may result in arbitrary jailing, especially for those computer professionals.[487] Unauthorised access or even alteration is widespread in the computer professionals, such as testing software and the security of computer system. Nonetheless, programmers do not regard their behaviours as a violation of the law because they intend to enhance cyber security rather than destroying it. However, such acts are subject to the discretionary power of the law enforcement agencies because the professionals indeed intentionally secured access to computers, and may also occasionally lead to damage. Therefore, a cyber-specific offence may also cover their behaviours.[488]

The third reason is regarding the judicial resources. Namely, the over-reaching federal law would arm the federal prosecutors dramatically, and the subsequent huge amount of prosecutions they bring would flood the federal courts.[489] The worry of over-reaching federal legislation and law enforcement agencies is neither new nor unique in the field of criminal law in the US. The Congress expanded the federal criminal jurisdiction to violent street crimes in the mid-1990s, leading to a debate on the expansion of the federal government's power.[490] Such expansion in the US is called over-federalisation. The over-federalisation, criticised by scholars, would grant the federal prosecutors huge discretionary power and allow them to charge and pursue cases no matter how minor they are. As a consequence, the federal courts would become over-loaded and their functions may thus be paralysed.[491]

---

[486] *Federal Computer Systems Protection Act (S. 1766), Hearing before the Subcommittee on Criminal Laws and Procedures, Comm. of the Judiciary*, 95th Cong., 2d Sess. (1976).

[487] See e.g. Charlotte Decker, 'Notes, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime', *Southern California Law Review,* vol. 81 (2008): 959-1016.

[488] *Ibid*.

[489] *Ibid*, p. 1003.

[490] Harry Litman and Mark D. Greenberg, 'Dual Prosecutions: A Model for Concurrent Federal Jurisdiction', *The ANNALS of the American Academy of Political and Social Science,* vol. 543 1(1996): 72-84.

[491] See *ibid*. See also Sanford H. Kadish, 'Comment: The Folly of Over-federalization', *Hastings Law Journal,* vol. 46 4(1994): 1247-1251.

4.2.2.2 Arguments for a cyber-specific legislation

Although many scholars oppose a specific law on computer crimes, the Congress chose to enact a new statute and have amended it several times to keep up with the developments of technology. Arguments on this side include the inadequacy of traditional criminal law in cyber context, the various reactions to computer crimes of individual states, to protect the financial interests, and to enhance the national security.

The first reason for a specific legislation is the inadequacy of applying traditional criminal provisions in cyber context. As argued, computer crimes are 'inherently different' from other criminalities, and therefore they constitute a new category of criminal conduct. Nonetheless, the traditional laws were drafted long before the appearance of computer, and were drafted without any prediction of the involvement of computers. For this reason, for the first the judiciary organs hesitate to apply the traditional laws to cyberspace, and for the second the applicability of traditional provisions are decided by accidental elements. For instance, as the case *United States v. Seidlitz* shows, if the offence was not committed across state border, the offender would escape from being punished. In addition, if judges insisted on stretching the traditional legislations to cyberspace, those who acted across the state border would be incriminated; while those who acted within state border would not, even though the *actus reas* and *mens rea* of the two acts are the same. Such situation is undoubtedly unfair both for the actor and for the people who suffered. Thus, the non-computer-specific laws were inappropriate to apply to computer crimes.[492]

The second reason rests on the states' reaction to computer crimes. 'Isolated attempts by state legislatures to deal with the problems signal a growing awareness of the need to address [the computer crime] issue.'[493] In the beginning, a few states, such as Ohio and Alaska, amended their traditional criminal law to cover abuses targeting or facilitated by computers, and incorporated computer (-related) crimes into existing criminal law.[494] Some other states, such as Florida and California, enacted new legislation to criminalise unauthorised access.[495] On the one hand, the state legislations raised the consensus on the inadequacy of stretching

[492] See Joseph M. Olivenbaum, '<Ctrl> <Alt> <Del>: Rethinking Federal Computer Crime Legislation', *Seton Hall Law Review,* vol. 27 (1997): 574-641, pp. 591-592.

[493] John Roddy, 'The Federal Computer Systems Protection Act', *Journal of Computers, Technology and Law,* 7(1976): 343-365, p. 365.

[494] See Richard C. Hollinger and Lonn Lanza-Kaduce, 'The Process of Criminalization: The Case of Computer Crime Laws', *Criminology,* vol. 26 1(1988): 101-126, pp. 103-104.

[495] *Ibid*.

traditional criminal provisions on cybercrime, if they are not inapplicable at all. On the other hand, there were inconsistencies among the laws of various states: certain conduct may count as criminality in California but not in Ohio.[496] In this situation, a uniform, comprehensive and far-reaching statutory response at the federal level was necessary to reduce computer crime and to solve the inconsistencies between states.[497]

The third argument, in response to the argument regarding civil liberties, rests on the concern over financial interests, namely, reducing the cost of computer crimes and protecting the development of electronic commerce.[498] In fact, the cost of computer crimes has long been pointed out in the Senate Report 1979. It was maintained in that report that computer crimes occurred at great cost to society. The huge expenses of individual victims caused by computer crimes and that of big corporations and the government on security measures may astonish everyone.[499] The society as a whole for the first suffered significant loss because of cybercrime, and for the second spent a huge amount of money on updating security measures in order to prevent cybercrime. Powerful federal legislation can help reduce computer crimes and thus cut expenses as such.[500] In addition, the US has gradually noticed the significance of a secured network to electronic commerce and the huge profits it can bring. Thus, the US should tighten its cybercrime legislation in order to promote electronic commerce. Just as an American expert addressed in the Council of Europe's Parliamentary Meeting, 'laws are needed to make cyber space safe, and countries with inadequate laws will be less competitive in the new economic markets.'[501]

Fourthly, taking a panoramic view of the amendments in history, to enhance national security has served as the main motivation behind. Taking the term of 'protected computers' as an example. In the CFAA 1984 the term 'federal interest computer' mainly refers to computers that exclusively used by the Government or financial institutions. After the Amendment 1986,

---

[496] Susan Hubbell Nycum, 'The Criminal Law Aspects of Computer Abuse: Part I State Penal Laws', *Journal of Computers and Law,* vol. 5 (1976): 271-295.

[497] John Roddy, 'The Federal Computer Systems Protection Act', *Journal of Computers, Technology and Law,* 7(1976): 343-365, p. 365.

[498] See e.g. Michael Hatcher, Jay McDannell and Stacy Ostfeld, 'Computer Crimes', *American Criminal Law Review,* vol. 36 (1999): 397-444, p. 436.

[499] Michael M. Krieger (compiled), 'Current and Proposed Computer Crime Legislation', *Compute/Law Journal,* vol. II Appendix(1980): 721-771, p. 722.

[500] Sara L. Marler, 'The Convention on Cybercrime: Should the United States Ratify?' *New England Law Review,* vol. 37 1(2002): 183-219, pp. 211-212 (mentioning that according to a survey in 2002, 85% of United States businesses had been hacked).

[501] *Ibid*, pp. 190-191.

if computers involved in an offence were more than one, and not all of them located in one state, they were also 'federal interest computers'. This amendment was to enhance the protection of states' security. Starting from the NIIPA 1996, the scope of 'protected computer' had already been broadened compared with the prior term of 'federal interest computer', and every computer in the United States arguably fell in the scope of 'protected computer'. The PA 2001 expanded the 'protected computers' to those even outside of the US. The ITERA 2008 further arguably brings all computers in the world under the federal jurisdiction of the United States.[502]

Lastly, sharing the concern about over-prosecution and the courts' workload, the Congress decided that computer trespass and computer misuse that result in more severe damages, should be treated differently, in order to avoid the excessive use of the specific Act. According to the Congress, the law should focus on those computer crimes that would 'either result in economic harm or threaten the integrity of sensitive data'.[503] Therefore, the Congress differentiates between misuse and felonies in the CFAA. For instance, all the requirements in the list of harm signal a clear distinction between acts punishable as a felony and punishable as a misdemeanour.[504]

Generally speaking, the enactment of a specific legislation indicates the Congress's position towards the debate on the necessity of such a statute. Moreover, the Congress started to discuss and draft this specific legislation on cybercrime as early as in the 1970s. It seems that the Congress does not believe judges could make far-reaching interpretations of traditional provisions into cyber context, and they thus needed guidance from new legislation. Some others believe that the Congress intended to use this legislation to educate netizens 'how to conform their behaviour' in cyberspace.[505]

The balance between online freedom and control over cyberspace used to incline to the former, reflected by the intentionally limited scope of the CFAA 1984. However, this balance inclined to the latter afterwards, driven by the financial profits and national security. Interestingly, the amending process of the CFAA shows the arguments against a

[502] See Orin S. Kerr, 'Vagueness Challenges to the Computer Fraud and Abuse Act', *Minnesota Law Review,* vol. 94 (2009): 1561-1587, pp. 1569-1570.

[503] Reid Skibell, 'Cybercrimes and Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act', *Berkeley Technology Law Journal,* vol. 18 (2003): 909-944, p. 912.

[504] *Ibid.*

[505] Jo-Ann M. Adams, 'Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet', *Computer and High Technology Law Journal,* 12(1996): 403-434, p. 419.

cyber-specific Act to be well-targeted: the concern over constant amendments is illustrated by the eight Amendments, and the worry on arbitrary jailing was exemplified by the legislation that 'recklessness' to the damage is criminalised.

4.3 Current Legislation on Cybercrime

4.3.1 Offences against the security of computer

Offences under this category include access offences, impairment of data, misuse of devices, and interception of data.

4.3.1.1 Access offences

The offences concerning hacking in the US contain a range of offences under different articles (18 U.S.C. § 1030(a)(1)-(3)), thus five constitutive elements are examined below rather than showing each relevant article in detail. The five elements are generalised by Jonathan Clough, including 'computer', 'access', 'authorisation', 'fault element' and 'additional element'.[506]

(1) Computer

Knowing that a narrow definition would always be challenged by the development of information technology, the US chose to grant an all-inclusive definition of 'computer'. In the 18 U.S.C. § 1030(e)(1), 'computer' is defined as

> 'an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device'.[507]

One advantage of such an exhaustive definition is certainty. In other words, the status of certain devices is clarified in this definition to avoid ambiguity.[508] For instance, from this definition the audience can easily know that a USB stick or a PDA belongs to computer, and is thus protected by the CFAA. The other advantage of an all-inclusive definition is the flexibility it brings, which can help fill gaps presented by the changing technologies. One

[506] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 51.

[507] 18 U.S.C. § 1030(e)(1).

[508] Joseph M. Olivenbaum, '<Ctrl> <Alt> <Del>: Rethinking Federal Computer Crime Legislation', *Seton Hall Law Review,* vol. 27 (1997): 574-641, pp. 619-621.

persuasive example of the flexibility is the subject of the access offences. Under the CFAA, merely the computer is protected, but not computer network, which makes judges daunting to apply the CFAA to acts damaging computer networks. The broad definition of 'computer' solves this problem. According to the definition, 'computer' includes 'a communications facility directly related to or operating in conjunction' with computers. Therefore, not only computer networks, but also the facilitating devices for communications such as a router belong to 'computer', and are thus protected under the CFAA.[509]

However, the disadvantage of a broad definition is over-inclusiveness, which comes together with certainty and flexibility. Certainty is difficult to maintain and short-lived in such a fast developing area. To provide certainty, any definition must be 'sufficiently precise', and need to be flexible enough to adapt to the never-ending evolution of computer crime at the same time. These conflicting aims of to be 'broad', 'sufficiently precise' and 'flexible' raise the problem of being over-inclusive.[510] This is the disadvantage of an exhaustive definition. To avoid this disadvantage, some digital devices are explicitly excluded, for instance, 'an automated typewriter or typesetter, a portable handheld calculator, or other similar device'. Although this exclusion may resolve this problem to some extent, legislative guidance to judges with respect to the devices that cannot be regarded as computer is necessary.[511]

(2) Access

Since the term 'access' is left undefined in the statute, the academia and the judicial organs cannot reach a consensus on the circumstances in which access is gained.[512] Basically, the courts and legal scholars especially discussed two perspectives of addressing this issue:

---

[509] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 58.

[510] *Ibid*, p. 56.

[511] *Ibid*, pp. 56-57.

[512] See Orin S. Kerr, 'Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Act', *Public Law and Legal Theory Research Paper Series Research Paper* No. 65 (2003): 1596-1668. This article provided several opinions regarding different perspectives for determing 'access'. Firstly, the 1977 BFCSPA stated that 'access means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network'. This definition, however, was criticised by the Department of Justice because '[this] approach is a physical concept and appears to include being close to a computer'. Secondly, courts of different states held different positions on this issue. In the *State v. Allen* case trialled in the Kansas Supreme Court, the judges adopted a narrow definition of 'access' and maintained that Allen had repeatedly dialled up the Bell computers and viewed the password prompt. The court found the statutory definition too broad and ruled that Allen did not gain access to the computer system 'as gaining access is commonly understood'. Nonetheless, in an almost identical case happened in *State v. Riley* case trialled in Washington Supreme Court, the defendant Riley was found to have repeatedly dialled the Telco access number and guessed passwords (the prosecutor could not prove whether he had guessed correctly and placed free calls). With the same statutory definition of access, the court found the defendant committed access by 'viewing computers as virtual spaces and accessing the computer as akin to getting inside the space'.

internal perspective and external perspective, referring to virtual perspective and physical-world perspective.[513]

The internal perspective, or virtual perspective, as explained by Jonathan Clough, is from the literal sense. To be specific, 'any interaction with the computer by way of inputs' is using that computer.[514] From this perspective, it does not matter whether the actor goes further with the access and gains information. As long as the input causes the computer to respond, no matter the response is the desired one or not, an access is successfully gained. A hacker who tried to get full access to a computer while failed would still meet the constituent element of 'access'. That means, mere hacking[515] is an offence under this approach.

The external perspective can also be referred to as the physical-world perspective. It means that the user sent a command to the computer and received the desired response.[516] Under this approach, the actor must 'make use of the computer in the sense of obtaining the use of programs or data'.[517] In other words, the offender uses the computer as a tool to provide him with certain facilities.[518] Therefore, a certain function of a computer must be evoked and used to perform the access.[519] In this regard, the hacker who failed to gain full access to a computer will fall out of 'access' because no function of the computer has been used.

Comparing these two perspectives, the real difference between them is the subject, or, interest, protected under the CFAA. The internal approach starts from protecting data; therefore, since any access will inevitably result in interaction with the computer, and interaction with the computer will change the data stored on the targeted computer, any access may damage the protected data, and thus violates the CFAA. The external approach, on the contrary, protects the computer. From this perspective it is the usage of the computer that is explored unauthorised, such as the computing capability and storage capability. In this sense, if an

[513] See Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, pp. 65-68. See also Orin S. Kerr, 'Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Act', *Public Law and Legal Theory Research Paper Series Research Paper* No. 65(2003): 1596-1668, p. 1621.

[514] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 68.

[515] Mere hacking in this dissertation is referred to as the situations where hacker does not change, delete, copy or other operate of any data without authorization when obtaining access.

[516] Orin S. Kerr, 'Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Act', *Public Law and Legal Theory Research Paper Series Research Paper* No. 65(2003): 1596-1668, p. 1621.

[517] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 69.

[518] Orin S. Kerr, 'Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Act', *Public Law and Legal Theory Research Paper Series Research Paper* No. 65(2003): 1596-1668.

[519] *Ibid*.

actor merely obtained access to get some data and he did not use the computer, he does not violate the CFAA, because the value and the function of the targeted computer suffer no damage.

Moreover, one can see that the internal perspective sets a wider criminalising net than the external perspective. With respect to the issue that which perspective is more appropriate, there is no consensus. Orin Kerr, a supporter of the internal perspective, argues that 'access' should be defined as 'any successful interaction with the computer', which means that 'a user accesses a computer whenever the user sends a command to that computer that the computer executes'.[520] The rationale behind this broad perspective is to avoid 'technical and often arbitrary arguments about what constitutes access, and appropriately focus on the remaining elements, which determine whether the alleged conduct is in fact criminal'.[521]

Contrary to Kerr's opinion, the Congress chose the external perspective on understanding 'access'. 18 U.S.C. § 1030 (b) provides a legal ground for attempting to commit access offences. A natural thought based on this regulation concerning these attempted access offences would be that if a broad interpretation of access is adopted, there is little, if any, room left for attempted access. The only chance would be if the actor were caught at the keyboard and he was about to type in the password but was stopped before any typing was made. It can be seen from this that the US legislature chose a narrow approach – the external perspective.[522] Under this approach, mere hacking is punished as unfinished crime.

(3) Authorisation

There is no definition of 'authorisation' in the CFAA. As mentioned above, the US chose a narrow approach when understanding 'access'. In line with this choice, the hacking provisions focus on computers rather than specific data stored on the computers. Following this line it would be argued that as long as the actor has authorisation to a computer, he should not be liable for obtaining data that exceeds his authorisation.[523] However, the

[520] *Ibid*, pp. 1646-1647.

[521] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 69. See also Orin S. Kerr, 'Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Act', *Public Law and Legal Theory Research Paper Series Research Paper* No. 65(2003): 1596-1668, pp. 1647-1648.

[522] There is one exception with respect to the perspective of understanding 'access'. 18 U.S.C. § 1030(a)(4) adopts the internal perspective in order to protect government computers.

[523] Matthew Kapitanyan, 'Beyound Wargames: How the Computer Fraud and Abuse Act Should Be Interpreted in the Employment Context', *I/S: A Journal of Law and Policy*, vol. 7 1(2011): 405-454, p. 426.

judicial practice tells a different story. The key issue is how to understand and determine the term 'authorisation'.

The earliest and most important case regarding authorisation is *United States v. Morris*.[524] The factual ground for the prosecution is that Morris, as a graduate student at Cornell University and authorised to access to computer system of Cornell, programmed a 'worm' for computers that could spread across the Internet to illustrate security flaws in the systems. After he released this worm, it quickly spread out of control and in the end shut down the early Internet. Morris was charged under 18 U.S.C. § 1030 (a)(5)(A), the one prohibiting 'intentionally accessing a Federal interest computer without authorisation' that time, and was found guilty.[525]

On appeal, Morris argued that he did not gain access without authorisation because he did have the right to access several of the infected computers, especially the ones belong to Cornell University. Before coming to this claim, he distinguished between two types of abuse of authorisation: totally without authorisation and exceeding authorisation.[526] A Senate report supported Morris's argument and indicated a difference between accesses totally without authorisation and exceeding authorised accesses 'based on the difference between insiders and outsiders'.[527] Insiders are those with limited authorisation to access a computer such as employees, and outsiders are those with no right to access a computer such as hackers.[528] Considering the narrow approach taken by the Congress on the issue of 'access',

[524] *United States v. Morris*, 928 F.2d 504 (2nd Cir. 1991). In October 1988, Morris began to work on a computer program, later known as the Internet 'worm' or 'virus'. The goal of this program was to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered. On 2 November 1988, Morris released the worm from a computer at the Massachusetts Institute of Technology (MIT). MIT was selected to disguise the fact that the worm was produced by Morris, who was studying at Cornell. Morris soon discovered that the worm was replicating and re-infecting machines at a much faster rate than he had anticipated. Ultimately, many machines at locations around the country either crashed or became 'catatonic'. When Morris realised what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent reinfection. However, because the network route was clogged, this message did not get through until it was too late. Computers were affected at numerous installations, including leading universities, military sites, and medical research facilities. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000. Morris was charged under 18 U.S.C. § 1030(a)(5)(A).

[525] For more detailed information see http://www.loundy.com/CASES/US_v_Morris2.html. Last visited March 2016.

[526] As previously mentioned, 'exceeds authorised access' was added to the CFAA by the Amendment 1986.

[527] Orin S. Kerr, 'Cybercrime's Scope: Interpreting "Access" and "Authorization" in the Computer Misuse Act', *Public Law and Legal Theory Research Paper Series Research Paper* No. 65 (2003): 1596-1668, p. 1630.

[528] *Ibid*.

a narrow interpretation of 'without authorisation' should be adopted and thus Morris's argument could be well founded.

Some scholars and legislator expressed their opposition to the distinction between without and exceeding authorisation. According to them, the distinction reflects the concern that users who were authorised with some rights to access a computer would use those rights for further computer misuses.[529] However, it may serve as 'an absolute defence' to help actors escape from being punished.[530]

The Second Circuit also rejected Morris' argument. The court maintained that

> 'Congress was not drawing a bright line between those who have some access to any federal interest computer and those who have none. Congress contemplated that individuals with access to some federal interest computers would be subject to liability under the computer fraud provisions for gaining unauthorised access to other federal interest computers'.[531]

After this reasoning, the court introduced a standard to determine under what circumstances access was authorised - the intended function test – through stating that Morris did not use those computers 'in any way related to their intended function'.[532] In this regard, although Morris was authorised to use the computers or programs, he was not authorised to 'exploit weaknesses in the programs that allow [him] to perform unintended functions'.[533] Therefore, if a user exploits weaknesses in a program and thus uses it in an unintended way to access a computer, this access is 'without authorisation' in the US legal context.[534] Judging from this

---

[529] See S. Rep. No. 104-357 (1996), p. 4. This report emphasised that 18 U.S.C. § 1030(a)(3), which penalises access to government computers without authorization, 'only applies to outsiders who gain unauthorised access to Federal Government computers, and not to Government employees who abuse their computer access privileges to obtain Government information that may be sensitive and confidential'. In this sense, access that exceeds authorization and access that is without authorization could be differentiated.

[530] *Ibid*.

[531] *United States v. Morris*, 928 F.2d 504 (2nd Cir. 1991).

[532] Orin S. Kerr, 'Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Act', *Public Law and Legal Theory Research Paper Series Research Paper* No. 65(2003): 1596-1668, pp. 1631-1632.

[533] *Ibid*.

[534] It should be noted that three ways have been developed to interpret whether the actor has 'authorization' in the context of 'without authorization': agency-based theory, contract-based theory and code-based theory. In the author's view, these three theories do not solve the problem. The real problem is in fact regarding the legal interests protected by the CFAA; and the reason for this problem is the inconsistencies between the approaches of interpreting the CFAA. This issue will be discussed in detail in Chapter 7. For more details on these three tests, see Brandon Darden, 'Definitional Vagueness in the CFAA: Will Cyberbullying Cause the Supreme Court to Intervene?' *Southern Methodist University Science and Technology Law Review*, vol. XIII (2010): 329-358.

test and reasoning, the Second Circuit took a broad approached of interpreting 'without authorisation'.

However, this is not always what the judges think in the US. In the case *LVRC Holdings v. Brekka,*[535] the court concluded that since LVRC gave Brekka the authorisation to use the company computer, he had authorisation to obtain all company files. Therefore, no matter what he did after he obtained the files, until the employer rescinded his authorisation, he was held authorised to use the files.[536] It can be observed from this conclusion that a narrow interpretation of 'authorisation' was adopted. This finding is upheld by a more recent case *United States v. Nosal*[537] by the Ninth Circuit. In this case, the employee (defendant) used his authorised account to steal information for use in his new business before the employer

---

See also Samantha Jensen, 'Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail', *Hamline Law Review,* vol. 36 (2013): 81-138.

[535] *LVRC Holdings v. Brekka,* 581 F.3d 1127 (9th Cir.2009). LVRC operates Fountain Ridge, a residential treatment center for addicted persons. In April 2003 LVRC hired defendant Brekka to handle internet marketing as well as a number of other aspects of the facility. In August of 2003 Brekka and LVRC began discussing the possibility of Brekka purchasing an ownership interest in LVRC. Consequently Brekka emailed a number of LVRC documents to his personal email account and his wife's personal email account. Included in these documents were a financial statement for the company, LVRC's marketing budget, administrative reports for patients at Fountain Ridge, and notes Brekka took from a meeting with another Nevada mental health provider. Brekka also emailed a master admissions report to his personal email account, which included the names of past and current patients at Fountain Ridge.

The discussions between Brekka and LVRC broke down and Brekka stopped working for the company in mid-September 2003. Brekka left his computer at LVRC and did not delete any email, including the email from the website administrator with his personal login information. Several other employees had access to Brekka's former computer before the login information was eventually deleted. In November 2004 the website administrator discovered that someone was logged ino the LVRC website using Brekka's former username and password. The login was traced to an Internet service provider (ISP) in Redwood City, California. The Brekka's former account was deactivated and LVRC filed a report with the FBI alleging unlawful access to their computer system. LVRC brought a claim against its former employee for allegedly violating the Computer Fraud and Abuse Act (CFAA). LVRC's complaint alleged that the employee violated the CFAA when he emailed LVRC documents to his personal email account and when he allegedly accessed the LVRC website after he stopped working for the company.

[536] *Ibid*.

[537] *United States v. Nosal*, 676 F.3d 854 (9th Cir.2012). From April 1996 to October 2004, Nosal worked as an executive for Korn/Ferry International (Korn/Ferry), an executive search firm. When Nosal left Korn/Ferry in October 2004, he signed a Separation and General Release Agreement and an Independent Contractor Agreement. Pursuant to these contracts, Nosal agreed to serve as an independent contractor for Korn/Ferry and not to compete with Korn/Ferry for one year. In return, Korn/Ferry agreed to pay Nosal two lump-sum payments in addition to twelve monthly payments of $25,000. Shortly after leaving his employment, Nosal engaged three Korn/Ferry employees to help him start a competing business. The indictment alleges that these employees obtained trade secrets and other proprietary information by using their user accounts to access the Korn/Ferry computer system. Specifically, the employees transferred to Nosal source lists, names, and contact information from the 'Searcher' database — a 'highly confidential and proprietary database of executives and companies' — which was considered by Korn/Ferry 'to be one of the most comprehensive databases of executive candidates in the world'. Nosal was charged under 18 U.S.C. § 1030(a)(4), under which 'knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorised access, and by means of such conduct furthers the intended fraud and obtains anything of value' is criminalised.

rescinded his authorisation.[538] The Ninth Circuit found the defendant non-guilty of the CFAA because the defendant was authorised to use the computer, and thus he did not violate the CFAA.[539]

It can be observed that the attitudes towards the perspective of understanding 'authorisation' differ from court to court, and from the judicial organs to the legislature. In fact, judges themselves had also noticed this divergence. The US Court of Appeals for the Ninth Circuit once pointed out:

> 'Some courts, including two courts of appeal, have broadly construed the CFAA to hold an employee acting to access an employer's computer to obtain business information with intent to defraud, i.e., for their own personal benefit or the benefit of a competitor, act "without authorisation" or "exceed authorisation" in violation of the statute. These courts have generally held that authorised access to a company computer terminated once an employee acted with adverse or nefarious interests and against the duty of loyalty imposed on an employee in an agency relationship with his or her employer or former employer.
>
> Other courts have refused to hold employees with access and nefarious interests within the statute, concluding that a violation for accessing a protected computer "without authorisation" or in "excess of authorised access" occurs only when initial access or the access of certain information is not permitted in the first instance. Those courts have generally reasoned that the CFAA is intended to punish computer hackers, electronic trespassers and other "outsiders" but not employees who abuse computer access privileges to misuse information derived from their employment.'[540]

Moreover, there is no consensus on the issue whether 'exceeds authorisation' should be distinguished from 'without authorisation'. Some argue that with this flaw the CFAA is nothing but a paper tiger;[541] some others have tried to develop measures and theories, the

---

[538] *Ibid*.

[539] *Ibid*.

[540] *United States v. Nosal*, 676 F.3d 854 (9th Cir.2012).

[541] Shawn E. Tuma, '"What Does CFAA Mean and Why Should I Care?" – A Primer on The Computer Fraud and Abuse Act for Civil Litigators', *South Carolina Law Review*, vol. 63 (2011): 141-189.

intended function test for instance, to determine whether a person is liable under the CFAA when he 'exceeds authorisation'.

(4) Fault element

In the United States the fault element of access offences is generally either 'knowingly' or 'intentionally'.[542] That means, an actor must know his conduct is unauthorised and he intends to do so, or he intentionally secures access to computers and causes damage.

One issue regarding fault element is whether the requirement of 'knowingly' or 'intentionally' applies only to 'access' or also applies to 'cause damage'. To be clearer, whether the defendant merely intends/knows the access is without or exceeding authorisation, or he must intends/knows the damage he would cause. If the former were the case, the actor's mental status to the consequence does not matter to determine whether he commits hacking offences. Therefore, a person may be held liable for behaviour where he inadvertently or recklessly caused damage, as long as he gained unauthorised access to the computer intentionally or knowingly.[543] If the latter were the case, the actor would not be held liable for the consequences he recklessly causes. For instance, in the aforementioned case *United States v. Morris,*[544] the defendant claimed that he intentionally spread the virus but inadvertently caused damage to the computers.

To determine on what occasions the actor has 'fault element', David Thaw, a legal scholar, proposed a reform towards the *mens rea* of the hacking offences: 'a two-part intent requirement'.[545] In his opinion, the actor must not only be intentionally and knowingly engaged in hacking offences, but also intend to further crimes either belonging to cybercrime

[542] The fault element in the US Criminal Code has changed several times ever since the birth of the CFAA. For these changes see the aforementioned historical review section. Acting 'intentionally' and acting 'knowingly' differ from each other. Firstly, knowingly accessing a computer…to obtain information protected for national security reasons and then disclosing it to unauthorised personnel is an offence under subsection 1030(a)(1). Intentionally accessing a computer ….to obtain either certain financial information, or information from a US government agency, or information from a protected computer where the conduct involved an interstate or foreign communication is an offence under subsection 1030(a)(2). Secondly, accessing intentionally and without authorization to any non-public computer of a department or agency of the US can be an offence under subsection 1030(a)(3). Thirdly, furthering a fraud by knowingly and with intent to defraud, accessing a protected computer without authorization, or exceeding authorised access is an offence under subsection 1030(a)(4). Mary W. S. Wong, 'Cyber-trespass and 'Unauthorised Access' as Legal Mechanisms of Access Control: Lessons from the US Experience', *International Journal of Law and Information Technology,* vol. 15 1(2006): 90-128, p. 116.

[543] See Haeji Hong, 'Hacking Through the Computer Fraud and Abuse Act', *UC Davis Law Review,* vol. 31 (1997): 283-307, pp. 290-294.

[544] *United States v. Morris*, 928 F.2d 504 (2nd Cir. 1991).

[545] David Thaw, 'Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement', *The Journal of Criminal Law and Criminology*, vol. 103 3(2013): 907-948, pp. 909-912.

or alternatively belonging to other crimes under the state or federal law.[546] This proposal, if accepted, may serve as a restriction against overbroad prosecutions since recklessness to damage is excluded.[547] The Congress seems not agree with him. Rather, the inclusion of 'recklessness' to consequences under 18 U.S.C. § 1030 (a)(5)(B) and (C) demonstrates the response to this issue from the legislature.

(5) Additional element

The CFAA has several additional elements in different provisions, focusing on 'harmful intent and resultant harm, rather than on the technical concept of computer access'.[548] For instance, 18 U.S.C. § 1030 (a)(1) states that '…access and by means of that access obtains and wilfully communicates specified protected information'. In this provision, 'obtaining information' is an additional element. It is used to ensure this provision has the maximum application without the debates that may arise if several overlapped provisions are mutually exclusive.[549] Other additional elements include 'protected computer' (18 U.S.C. § 1030(a)(2)(C)), 'US department or agency' (18 U.S.C. § 1030(a)(3)), 'non-public computer' (18 U.S.C. § 1030(a)(3)), and others.

4.3.1.2 Impairment of computer

The principal offence regarding the damage to computers, data and systems is found in 18 U.S.C. § 1030 (a)(5). Containing three different forms of impairing data, not only the mental status of 'intentionally', but also 'recklessly' and 'inadvertently' are incriminated.[550]

[546] *Ibid*.

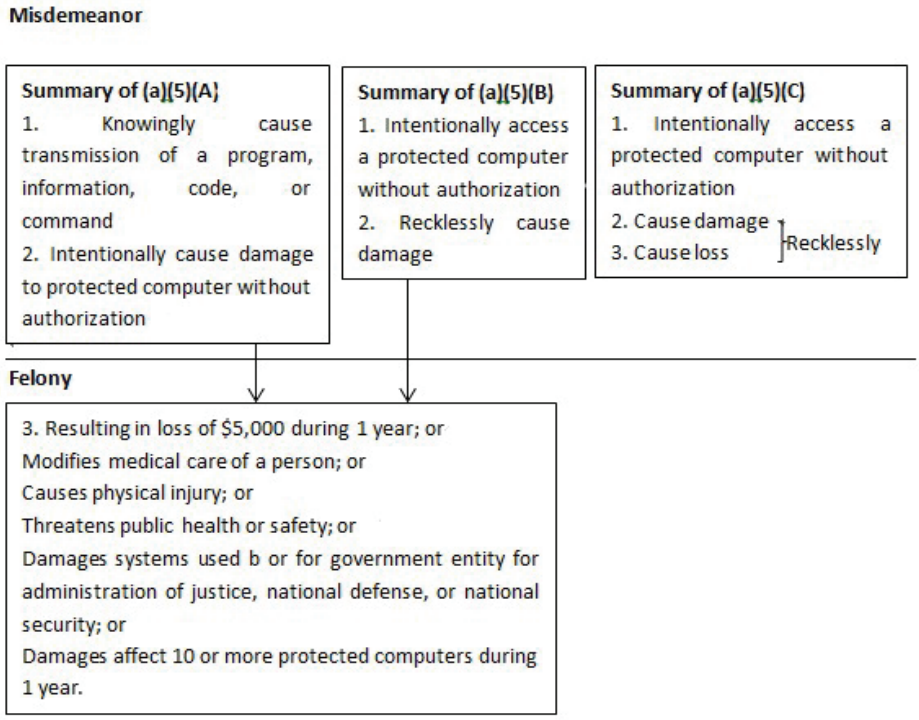
[547] *Ibid*.

[548] See Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 97.

[549] *Ibid*.

[550] See Figure 5.1 as a summary for these three forms.

Figure 5.1 Penalties of the impairment of computer



(Source: Prosecuting Computer Crimes, Computer Crime and Intellectual Property Section Criminal Division, Published by Office of Legal Education Executive Office for United States Attorneys (2010))

The Figure 5.1 clearly shows that the fault elements of these subsections differ - a main distinction among them. Under (a)(5)(A) the transmission must be conducted knowingly, and the damage must be caused intentionally. If the actor transmitted a program, information, code or command knowingly yet did not mean to cause the resultant damage, he shall not be liable under this offence.[551] Under the next two subsections, even if the actor recklessly causes damage, he shall be punished when other requirements are met.

The second distinction among these three forms is the subject of authorisation. While it is required to be 'without authorisation' before constituting all these three forms, the subject of authorisation is distinguished. Under (a)(5)(A), the causing of damage (e.g. delete data) must

[551] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 105.

be unauthorised, as indicated by the wording of (a)(5)(A). In this regard, even if the transmission is authorised, the actor may still be liable if the causing of damage is not; or if the transmission is not authorised, but the causing of damage is, the actor shall not be liable.[552] For instance, the actor has authority to use the computer editing word documents, but he deleted the OFFICE software and the computer could not open word documents anymore. He shall be punished under (a)(5)(A). As for the other two forms, the access *per se* must be without authorisation.[553]

Lastly, all of the three forms of the impairment of computers must be conducted without authorisation. However, the term 'without authorisation' may possess different meanings. Considering the wording used in subsections (a)(2) and (a)(4) that offences shall be committed 'without authorisation or exceeds authorised access', 'without authorisation' and 'exceeds authorised access' refers to different situations. In this sense, the impairment of computer arguably can only be committed without authorisation. However, the Computer Crime and Intellectual Property Section Criminal Division explains that (a)(5)(A) 'applies equally to offenders who are authorised to use the victim computer system, to those not authorised to use it, and to those who have never accessed the system at all';[554] while subsections (a)(5)(B) and (C) shall not apply to authorised users who exceed their authorisation.[555]

4.3.1.3 Misuse of devices

The offences relating to misuse of devices are penalised under 18 U.S.C. § 1029 and 18 U.S.C. § 1030(a)(6), regulating fraud and related activities in connection with access devices and trafficking in passwords.

(1) 18 U.S.C. § 1029 *fraud and related activity in connection with access devices*

Listing more than ten separate subsections to incriminating fraud and related offences under section 1029, the range of section 1029 has caused heated discussion ever since its birth in the 1970s and especially intensively after technical advances in the 1980s. Section 1029

[552] *Ibid*.

[553] *Ibid*.

[554] *Prosecuting Computer Crimes*, Computer Crime and Intellectual Property Section Criminal Division, Published by Office of Legal Education Executive Office for United States Attorneys, 2010, p. 37.

[555] *Ibid*, p. 38.

targets activities that produce, use, traffic or possess counterfeit access devices or device-making equipment.[556]

Initially, the purpose of section 1029 was to criminalise credit card abuses. Therefore, the concept 'access device' under this section was defined in connection with credit card abuses. Since it was drafted without any foresight of technical advances in the next decades, it was proved improper in a digital age.[557] In this context, the term 'access devices' has been reinterpreted in a way that should be 'broad enough to encompass technical advances' by the Fifth Circuit when deciding *US v. Brewer*.[558] Through reinterpreting this term, section 1029 can apply to fraud and other related activities that in relation to computers, data and programs.

(b) 18 U.S.C. § 1030(a)(6) *trafficking in passwords*

This subsection prohibits acts that

> 'knowingly and with intent to defraud traffics in any password or similar information through which a computer may be accessed without authorisation, if
>
> (A) such trafficking affects interstate or foreign commerce; or
>
> (B) such computer is used by or for the Government of the United States'.[559]

This subsection refers to passwords and 'similar information'. Firstly, this section only applies to information, not to a computer. Secondly, such information must be similar to a password and serve a function through which 'a computer may be accessed without authorisation'. In this regard, one issue rises: whether software or malicious code counts as 'information'. There are cases where actors used software or malicious code to break through the computers' security measure, and then gained access to a computer. In this situation, the

---

[556] According to 18 U.S.C. § 1029(e)(1), 'access device' is defined as 'any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)'.

[557] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 130.

[558] *United States v. Brewer*, 835 F 2d 550, 553 (5th Cir. 1987). On appeal the defendant argued that Congress did not intend to reach misuse of telephone access codes for 18 U.S.C. § 1029. The appeal court rejected this argument and expressed that 'we are persuaded that Brewer's conduct is reached by a practical reading of the statute. Both the Senate and House Reports on the statute state that the definition of 'access device' was intended to be 'broad enough to encompass technological advances'.

[559] 18 U.S.C. § 1030(a)(6). Accordign to 18 U.S.C. § 1029(e)(5), the term 'traffic' refers to 'transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of'.

software or malicious code is the device to secure access to a computer without right, while is arguably not similar to a password. Then, are they 'password'? To answer this question, the definition of 'password' should be investigated. There is no definition of 'password' in the CFAA. Fortunately, the one provided by the Office of Legal Education Executive Office for United States Attorneys can provide some guidance. According to it,

> 'a password may actually be comprised of a set of instructions or directions for gaining access to a computer and intends that the word password be construed broadly enough to encompass both single words and longer more detailed explanations on how to access others' computers'.[560]

Analysing from this definition, the authority intends to define and interpret 'password' broadly so as to cover all words, programs, codes or data that can be used to access computers. Therefore, software or malicious code may constitute 'similar information'.

As previously discussed, the CFAA protects computers rather than data; thus mere hacking is not a complete computer misuse. Following this rationale, trafficking in information that can be used to access without authorisation should not be a crime either. Or at least, it is not a complete crime but the preparation of the hacking offence, because it is actually the provision of criminal tools. However, the US legislators criminalise it and treat it as a complete crime, which in fact contradicts the approach the US takes.

4.3.1.4 Interception of communication and data

There is no offence as interception of data in the US legal system as in the Convention on Cybercrime. Instead, the corresponding offences are interception of contents and access to stored data. In addition, these offences are not prescribed by the CFAA. Rather, they are listed in mainly two statutes. They are interception of contents[561] in the Wiretap Act (hereafter the USWA, 18 U.S.C. § 2511) subsection (1)(a),[562] and access to stored communications in the Stored Communications Act (hereafter the USSCA, 18 U.S.C. § 2701) subsection (a).[563]

---

[560] *Prosecuting Computer Crimes*, Computer Crime and Intellectual Property Section Criminal Division, Published by Office of Legal Education Executive Office for United States Attorneys, 2010, p. 50.

[561] 'Contents' here used to refer to 'any wire, oral, or electronic communication, and it includes any information concerning the substance, purport, or meaning of that communication'. 18 U.S.C. § 2510(8).

[562] 18 U.S.C. § 2511(1)(a).

[563] 18 U.S.C. § 2701(a) makes it an offence where a person (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an

Comparing these two offences, the main difference is their subject, namely, contents and stored communication, and 'contents' mainly refer to wire communication. The difference between wire communication and stored communication is relatively clear. Wire communication mainly refers to the communication made by the aid of wire, cable, or other like connection. Namely, 'wire communication' is

> 'any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce'.[564]

Further, a House Report sets a rule that distinguishing these two on the basis of 'sound waves' or 'human voice'. The rule is

> '[A stored] communication is an electronic communication if it is neither carried by sound waves nor can fairly be characterised as one containing the human voice (carried in part by wire). [Stored] Communications consisting solely of data, for example…would be electronic communications'.[565]

4.3.2 Traditional crimes facilitated by computer

Taking the framework of the Convention on Cybercrime, offences under 4.3.2 include computer fraud and forgery, child pornography and copyright related cybercrime.

4.3.2.1 Computer facilitated fraud and forgery

18 U.S.C. § 1343 (wire fraud statute) and 1030(a)(4) are provisions that dealing with computer-related fraud in the US. Namely, under section 1343, 'whoever, having devised or

---

authorization to access that facility. Thereby obtains, alters, or prevents authorised access to a wire or electronic communication while it is in electronic storage in such system shall be punished. A '*wire communication*' means any oral transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce (18 U.S.C. § 2510(1)). An '*oral communication*' is any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication (18 U.S.C. § 2510(2)).

[564] 18 U.S.C. § 2510(1).

[565] Cited in Peter J. Toren, *Intellectual Property and Computer Crimes*, New York: Law Journal Press, 2014, p. 8-54.

intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice' shall be punished. At the same time, under subsection 1030(a)(4) those who, knowingly and with intent to defraud, gain access to a protected computer without or in excess of authorisation, and by such conduct further the intended fraud and obtain anything of value shall be punished.

Strictly speaking, these two offences mainly differ in the way they are conducted. The wire fraud is committed by means of wire, radio or television communication; while computer-related fraud is committed through access to protected computers. Nonetheless, computer data is transmitted through wire, and computer-related fraud is for most possibility committed through network, which is also established through wire. Thus, it seems that these two offences are overlapped on certain circumstances. Sharing the same concern, legislators have emphasised that committing fraud through obtaining access to a computer is the key characteristic of computer-related fraud. One Senate said in a Senate Report that compared with wire fraud, the use of a computer must be more directly linked to furthering the intended fraud in computer-related fraud.[566] Besides, legislators maintain that subsection 1030(a)(4) should apply to those who attempt to steal valuable data through unauthorised access 'as part of an illegal scheme'.[567]

However, in judicial practice these two offences still overlap to a substantial degree. Computer-related fraud should in principle be regulated under subsection 1030(a)(4); while most of computer-related frauds are committed through making use of a 'wire', to which section 1343 can also apply. For instance, the courts have applied section 1343 to a variety of computer-related fraud cases and situations, such as making an airline reservation with a stolen credit card online in the case *US v. Drummond*[568] and using the Internet to commit fraud in the case *US v. Pirello.*[569]

---

[566] S. Rep. No. 99-432 (1986), p. 9.

[567] *Ibid*.

[568] *United States v. Drummond,* 255 Fed. Appx. 60, 64 (6th Cir. 2007). This prosecution arises from an ill-advised flight that defendant and his friend, Alesha Banks, planned to take from Flint, Michigan to New York City on 14 October 2005. The security department of AirTran Airways, the carrier on which the couple planned to fly, flagged the transaction as worth investigating because defendant booked the tickets online and paid with a credit card issued in the name of Bob Curlee, a Georgia resident. When contacted, Curlee indicated that he had not booked the flight. Further investigation revealed that defendant had booked rooms online at a hotel in New

In this context, to further emphasise the involvement of computer of the computer-related fraud, the Office of Legal Education provide a list that on what occasions a computer 'furthers' the fraud. The list contains

> 'alters or deletes records on a computer and then receives something of value from an individual who relied on the accuracy of those altered or deleted records;
>
> obtains information from a computer and then later uses that information to commit fraud; and
>
> uses a computer to produce falsified documents that are later used to defraud'.[570]

4.3.2.2 Offences related to child-pornography

The CFAA does not introduce an offence as computer-related child pornography. Instead, the US statutes relating to child pornography include 18 U.S.C. § 2251 (penalising sexual exploration of children), 2251A (prohibiting selling or buying a minor for producing child pornography), 2252 (prohibiting possessing, distributing and receiving child pornography), 2252A (issues relating to materials constituting or containing child pornography), 2256 (definitions) and 2260 (relating to jurisdiction abroad).

Section 2256 defines child pornography as 'any visual depiction of sexually explicit conducts involving a minor', and 'a minor' means those under 18 years' old.[571] For the meaning of

---

York for three days using another card in someone else's name. Once again, the cardholders, residents of Virginia, knew nothing of the transaction. At the airport, defendant and Banks checked three bags before proceeding to the gate. Thereafter, they were paged to return to the ticket counter based upon an alert from AirTran security. Ticket agent Laurin Malone reviewed their identification and asked the pair to wait at the counter while she spoke to a supervisor who instructed Malone to photocopy the identification. Accordingly, Malone asked for their identification a second time after she returned to the counter.

The defendant was convicted of two counts: wire fraud and possession of fifteen or more credit card numbers with the intent to defraud, under 18 U.S.C. § 1029(a)(3) and 1343 respectively. Available at https://casetext.com/case/us-v-drummond-4?passage=jfQph-Vg1WAKViXVjOi0Tg. Last visited April 2016.

[569] *United States v. Pirello,* 255 F 3d 728 (9th Cir. 2001). During the fall of 1999, Pirello placed four separate advertisements on an Internet classified-ads website, each soliciting buyers for a different type of computer. The website, known as Excite Classifieds, allows individuals to post classified-ads that can be readily accessed by the general public. The advertisements posted by Pirello were part of a fraudulent scheme whereby Pirello would induce prospective buyers to send him money for computers he never intended to deliver. Between October and December of 1999, three individuals responded to Pirello's fraudulent Internet advertisements. Pirello negotiated the sale of a computer to each of the three individuals, assuring them that the computers would be delivered upon his receipt of their payments. Pirello received over $4,000 in checks for the non-existent computers, which he deposited into his personal bank account. When Pirello's victims did not receive their computers as promised, they immediately contacted the FBI. Pirello admitted to the FBI that he had received several large checks from various individuals, but professed ignorance as to why he had been sent the money. Pirello was charged in a superseding indictment with three counts of wire fraud and three counts of mail fraud. Later he pled guilty to three counts of wire fraud in violation of 18 U.S.C. § 1343.

[570] *Prosecuting Computer Crimes*, Computer Crime and Intellectual Property Section Criminal Division, Published by Office of Legal Education Executive Office for United States Attorneys, 2010, p. 30.

'sexually explicit conduct', the US replicates the definition found in the CoC. Namely, it means 'actual or simulated (1) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (2) bestiality; (3) masturbation; (4) sadistic or masochistic abuse; or (5) lascivious exhibition of the genitals or pubic area of any person'.[572] With respect to the meaning of 'lascivious exhibition', courts have considered criteria that 'whether the focal point of the visual depiction is on the child's genitalia or pubic area, whether the setting is sexually suggestive, whether the child is depicted in an unnatural pose or inappropriate attire, whether the child is fully or partially clothed, or nude, whether the visual depiction suggests sexual coyness or a willingness to engage in sexual activity, and whether it is intended or designed to elicit a sexual response in the viewer'.[573]

4.3.2.3 Offences related to infringements of copyright and related rights

Similar to child pornography offences, the CFAA does not introduce offence on copyright related computer crimes either; rather, such acts are dealt with under 17 U.S.C. § 506. Under this section,

> 'any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed –
>
> (A) for purposes of commercial advantage or private financial gain;
>
> (B) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phone-records of 1 or more copyrighted works, which have a total retail value of more than $1,000; or

---

[571] 18 U.S.C. § 2256(1) and (8).

[572] 18 U.S.C. § 2256(2). As an exception, for the purpose of subsection 8(B) of section 2256, 'sexually explicit conduct' means

(1) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited;

(2) graphic or lascivious simulated;

(I) bestiality;

(II) masturbation; or

(III) sadistic or masochistic abuse; or

(3) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

[573] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 261.

> (C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution.'[574]

Before going further to introduce the legislation on copyright infringements facilitated by computer, it is worth noting that arising from the US Constitution, Copyright Law can only be enacted at federal level, meaning that states do not have the authority to legislate in this field.[575]

The purpose for 'commercial' profit is a requirement of this offence. Subsection (a)(1)(A) proscribes the act that engages in willful infringement for the purpose of *commercial* advantage or for private financial gain.[576] The case *US v. LaMacchia*[577] is the one in point. The defendant set up two servers to store files that other computers could access. He then invited Internet users to upload copyrighted software onto one server and to take copies of copyrighted software from the other, freely. Because the defendant did not do this for profit, the copyright statute did not prohibit his acts. Therefore, the jury acquitted him.

---

[574] 17 U.S.C. § 506(a)(1).

[575] See Susan W. Brenner, 'U.S. Cybercrime Law: Defining Offences', *Information Systems Frontiers,* 6(2004): 115-132, p. 120. Towards the nature of copyright, some argue that copyright falls into the ambit of intellectual property, thus constituting property. Others maintain that copyright is not property at all, but a limited statutory monopoly. The Supreme Court made this issue clear by stating that copyright is a limited statutory monopoly granted by Congress pursuant to the Constitution and not a nature law right of the creator of a work. See Lydia Pallas Loren, 'Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and the Importance of the Wilfulness Requirement', *Washington University Law Quarterly,* vol. 77 (1999): 835-899, p. 856.

[576] Lydia Pallas Loren, 'Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and the Importance of the Wilfulness Requirement', *Washington University Law Quarterly,* vol. 77 (1999): 835-899.

[577] *United States v. LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994). The defendant, LaMacchia, a computer hacker, used the computer network of Massachusetts Institute of Technology (MIT) to gain entree to the Internet. Using pseudonyms and an encrypted address, LaMacchia set up an electronic bulletin board which he named Cynosure. He encouraged his correspondents to upload popular software applications (Excel 5.0 and WordPerfect 6.0) and computer games (Sim City 2000). He transferred these to a second encrypted address (Cynosure II) where they could be downloaded by other users with access to the Cynosure password. Although LaMacchia was at pains to impress the need for circumspection on the part of his subscribers, the worldwide traffic generated by the offer of free software attracted the notice of university and federal authorities.

A federal grand jury returned a one count indictment charging LaMacchia to violate 18 U.S.C. § 1343, the wire fraud statute in the first instance. Later the defendant brought a motion to dismiss, arguing that the government had improperly resorted to the wire fraud statute as a copyright enforcement tool. This motion was allowed by a district judge.

4.3.3 Jurisdiction

The US established *extraterritorial jurisdiction* in the CFAA.[578] As previously mentioned, a number of subsections apply to acts threatening a 'protected computer'. This term, according to its definition, is broad enough to grant the US criminal jurisdiction over computers used in a manner that affects 'interstate or foreign commerce or communication'. Considering the fact that the Internet is regarded as an instrument of interstate commerce,[579] any act that happened on the Internet would lead to an interstate effect, and therefore any computer connected to the Internet is arguably used in an interstate or foreign commerce or communication. This reasoning leads to a situation that in fact any act, as long as it was conducted through or targeted at a computer connected to the Internet, meets the requirement of affecting 'interstate or foreign commerce or communication'. For instance, in the case *US v. Trotter,*[580] the court held that 'the Internet is an instrumentality and channel of interstate commerce' and affirmed that the requirement of affecting 'interstate or foreign commerce or communication' was satisfied. In another case *US v. Sutcliffe,*[581] the court concluded that 'it is legally sufficient for the purpose of the "interstate commerce" requirement that the emails at issue were sent and received through the Internet'.

This situation results in a thorny problem that the CFAA in fact has jurisdiction over any act if it was conducted through or targeted at a computer connected to the Internet, no matter where the computer is or what nationality the actor is. That is, extra-territorial jurisdiction.

The extra-territorial jurisdiction can avoid situations where no country concerned can or would like to claim jurisdiction. In addition, it can enhance the protection of the US. As commented by judges, 'the intent to cause effects within the United States…makes it reasonable to apply to a person outside United States territory a statute which is not extra-territorial in scope.'[582]

However, a jurisdiction as broad as this cannot escape criticism. One main concern is that it may give rise to competing jurisdictional claims with other countries.[583] To solve such

---

[578] See *Prosecuting Computer Crimes*, Computer Crime and Intellectual Property Section Criminal Division, Published by Office of Legal Education Executive Office for United States Attorneys, 2010, pp. 113-116.

[579] *United States v. Runyan,* 290 F 3d 223. 239 (5th Cir. 2002).

[580] *United States v. Trotter,* 478 F 3d 918, 921 (8th Cir. 2007).

[581] *United States v. Sutcliffe*, 505 F 3d 944, 952 (9th Cir. 2007).

[582] *United States v. Muench*, 694 F 2d 28, 33 (2nd Cir. 1982).

[583] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 411.

competing jurisdiction, international Convention or multilateral and bilateral treaties can help. The Convention on Cybercrime establishes a system to determine the most appropriate jurisdiction.[584] Nonetheless, the US declares reservation on Article 24 and 27 of the CoC, two provisions with respect to international cooperation and mutual assistance. Therefore, the cooperation framework established by the Convention on Cybercrime is not applicable in the cases concerning US. Rather, the US established its international cooperation and mutual assistance mechanisms regarding the international response to cyber-security on the basis of the G8 subgroup on High-Tech Crime.[585]

4.4 The Scope of Cybercrime and the Attitude towards the CoC in the US

This section focuses on two topics, namely, the scope of cybercrime in the US and its attitude toward the CoC. The extent to which the term of 'cybercrime' should reach and be regulated has always been a hot topic. Since the US is a forerunner of using criminal law to regulating cyber wrongdoings, its discussion on this issue may provide insights on the proper scope of cybercrime. In addition, not being a member State of the Council of Europe, the US signed the Convention on Cybercrime right after it was open for signature. However, it took the US five years to ratify it. As an observer State, the US has taken part in the drafting and negotiation of the Convention as early as the 1980s, so as to ensure the CFAA meets the requirements of implementing the Convention.[586] The factors that hindered the US ratifying the CoC, together with the American attitude on the Convention, will be briefly examined.

4.4.1 The scope of cybercrime

Cybercrime in the US is treated neither as an entirely new phenomenon nor old crimes performed in new ways;[587] rather, it is regarded by legislators and scholars as both. For instance, the legislators have introduced offences relating to online theft and computer fraud with the CFAA, a specific law on computer misuse. Scholars hold the same opinion. By regarding crimes as social harms, they describe cybercrime as 'the use of computer

---

[584] Article 22(5) of the Convention on Cybercrime, the Council of Europe.

[585] See Jeffrey Hunker, 'U.S. International Policy for Cyber-security: Five Issues that Won't Go Away', *Journal of National Security Law and Policy*, 4(2010): 197-216, pp. 204-207. The US also establishes information multilateral cooperation system based on the Group of Eight Subgroup on High-Tech Crime.

[586] See *Frequently Asked Questions and Answers about the Council of Europe Convention on Cybercrime (Draft 24 REV2)*, 1 December 2000, available at http://archive.today/QHdXG. Last visited March 2015. Original website is no longer available now.

[587] See Susan. W. Brenner, 'Cybercrime Metrics: Old wine, new bottle?' *Virginia Journal of Law and Technology,* vol. 9 13(2004): 1-53, p.15.

technology to commit either (a) social harms that have already been identified and outlawed generally (trespass, burglary, theft, stalking, etc.), or (b) new types of social harm that do not fall into traditional "crime categories"',[588] such as hacking.

Accordingly, as suggested by the Department of Justice and legal scholars, cybercrime, contains three subgroups, two of them are echoing the abovementioned two kinds of social harms, and the last one is in which computer is an accidental element. Namely, these three groups are:[589]

1. Existing offences in which the computer is used as a criminal instrument. For example, e-commerce fraud, criminal intellectual property infringement and illegal interception.
2. Crimes where the computer or computer-network is the target. For instance, DoS or DDoS attack,[590] hacking (gain access to a computer system without authorisation), and aggravated hacking (gain access to a computer system without authorisation for the purpose of committing other crimes).
3. Crimes in which the use of the computer is an incidental aspect of the commission of the crime but may afford evidence of the crime. For example, addresses found in the computer of a murder suspect, or phone records of conversations between offender and victim before a homicide. In such cases the computer is not significantly implicated in the commission of the offence, but more a source of evidence.[591]

These three subgroups of cybercrime can be described as the genuine computer crime, computer facilitated/related crime[592] and computer supported crime.[593] The genuine computer crimes are those described as offences against the confidentiality, integrity and

---

[588] Susan W. Brenner, 'U.S. Cybercrime Law: Defining Offences', *Information Systems Frontiers*, 6(2004): 115-132, p. 116.

[589] See Sheridan Morris, 'The Future of Net-crime Now: Part 1-Threats and Challenges', *Home Office Online Report 62/04*, available at http://www.globalinitiative.net/download/cybercrime/europe-russia/Home%20Office%20-%20The%20future%20of%20netcrime%20now%20-%20Part%201%20%E2%80%93%20threats%20and%20challenges.pdf. Last visited March 2015. See also Jiang Ping, *计算机犯罪问题研究* (Research on Problems Involving Computer Crimes), Beijing: The Commercial Press, 2000.

[590] 'DoS attack (denial-of-service attack) or DDoS attack (distributed denial-of-service attack) is an attempt to make a machine or network resource unavailable to intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.' See more details on *Denial-of-Service Attack* at https://en.wikipedia.org/wiki/Denial-of-service_attack. Last visited March 2015.

[591] See Susan W. Brenner, 'U.S. Cybercrime Law: Defining Offences', *Information Systems Frontiers*, 6 (2004): 115-132, pp. 116-117. See also Computer Crime and Intellectual Property Section, US Department of Justice, *The National Information Infrastructure Protection Act of 1996*, Legislative Analysis (1996).

[592] Sheridan Morris, 'The Future of Netcrime Now: Part 1-Threats and Challenges', *Home Office Online Report 62/04*.

[593] M. Kowalski, *Cyber-Crime: Issue, data sources, and feasibility of collecting police-reported statistics*, Cat. No. 85-588, Canadian Centre for Justice Statistics, 2002, p.6.

availability of computer data and systems in the Convention on Cybercrime. Computer facilitated crimes are the traditional crimes facilitated by computer. The third subgroup is not explicitly mentioned in the CFAA; neither is it mentioned in the CoC. As commented, the third subgroup is arguably a category in theory rather than in practice;[594] while still, the Department of Justice regards it as cybercrime.

4.4.2 The American attitude towards the Convention on Cybercrime

As mentioned, although the US has taken part in drafting and negotiating the Convention on Cybercrime as early as the 1980s, it still took five years for the US to ratify the Convention. During this period, two interests are especially considered and balanced, they are: '(1) society's interest in protection from and prevention of crimes committed through the Internet and on computers, as well as society's demand for secure networks; (2) the interest of those who wish to maintain their civil liberties, such as privacy and free speech, while on the Internet, and protection against self-incrimination as well as fourth amendment search and seizure provisions'.[595] Before addressing the competition between these two interests, the role in drafting the Convention played by the US, as a non-member state of the Council of Europe, is worth mentioning.

Originally, the US, represented by the Department of Justice and the Department of State, was invited by the Council of Europe to participate as an 'observer' in 1989 and 1995 when drafting recommendations during this period. Based on considerations that the US was vulnerable to computer crimes and a well-drafted international legal instrument would benefit the US to combat them, it accepted the invitation and participated in the drafting and negotiating process. Because of its participation in this process, as a non-member state to the Council of Europe, the US could become a party to the Convention. Its participation in this process also ensured that most of the obligations and powers contemplated by the draft CoC had already been established in the US law, in order to make it less controversial to be implemented into the US domestic law.[596]

---

[594] As argued by Susan W. Brenner in her article, such crimes may need new laws to resolve procedural issues for prosecution.

[595] Sara L. Marler, 'The Convention on Cybercrime: Should the United States Ratify?' *New England Law Review,* vol. 37 1(2002): 183-219, p. 184.

[596] See *Frequently Asked Questions and Answers about the Council of Europe Convention on Cybercrime (Draft 24 REV2)*, 1 December 2000, available at http://archive.today/QHdXG. Last visited March 2015. Original website is no longer available now.

However, the subtle balance between society's interests and civil liberties hindered the ratification of the CoC. The lack of privacy protection in the Convention is the first issue US scholars discussed.[597] The opponents of the CoC are mostly supporters of civil liberties. They argued that more powers would be given to police if the state ratified it. For instance, the CoC requires Internet Service Providers to maintain information about their users, and to provide relevant information to the government when they are asked to do so in certain situations.[598] This requirement would have the potential of violating privacy rights of individual citizens. Consequently, this would assist the government to get access to private information. Furthermore, the possibility of abusing various fundamental rights, *inter alia*, search and seizure,[599] the due process and the protection against self-incrimination[600] would be increased.[601] The second concern is that Internet Service Providers would be held criminally responsible for failing to monitor customer or user content, or for the criminal

---

Although having ensured there was no substantive conflict between the CoC and the US domestic law through participating in the drafting process, the US still claims several reservations. Its reservations include (1) under the US federal law, the offences set forth in Article 2 of the CoC (illegal access) include an additional requirement of intent to obtain computer data; (2) under the US federal law, the offences set forth in paragraph (1)(b) of Article 6 of the CoC (misuse of devices) require that a minimum amount of items be possessed; (3) under the US federal law, the offences set forth in Article 7 of the CoC (computer-related forgery) requires an intent to defraud; (4) pursuant to Article 4, the US reserves the right to require that the conduct result in serious harm, which shall be determined in accordance with applicable federal law; (5) pursuant to Article 6, the US reserves the right not to apply paragraph (1)(a)(i) and (1)(b) of Article 6 with respect to devices designed or adapted primarily for the purpose of committing offences established in Article 4 (data interference) and Article 5 (system interference); (6) pursuant to Article 9, the US reserves the right to apply paragraph (2)(b) and (2)(c) of Article 9 only to the extent consistent with the US Constitution as interpreted by the US and as provided for under its federal law, which includes, for instance, crimes of distribution of material considered to be obscene under applicable US standards; (7) pursuant to Article 10, the US reserves the right to impose other effective remedies in lieu of criminal liability under paragraphs 1 and 2 of Article 10 (offences related to infringement of copyright and related rights) with respect to infringements of certain rental rights to the extent the criminalisation of such infringements is not required pursuant to the obligations the US has undertaken under the agreements referenced in paragraphs 1 and 2.

[597] See Mark Ward, Treaty 'Could Stifle Online privacy', *BBC News*, 11 June 2001, available at http://news.bbc.co.uk/2/hi/science/nature/1378482.stm. Last visited March 2015.

[598] See Sara L. Marler, 'The Convention on Cybercrime: Should the United States Ratify?' *New England Law Review*, vol. 37 1(2002): 183-219, p.203.

[599] Established in the Fourth Amendment of the United States Constitution.

[600] Established in the Fifth Amendment of the United States Constitution.

[601] See Sara L. Marler, 'The Convention on Cybercrime: Should the United States Ratify?' *New England Law Review*, vol. 37 1(2002): 183-219, p.202.

actions conducted by their employees.[602] That is, some one is liable for actions of the third party.[603]

Supporters of the CoC agree with neither of the arguments above. With respect to the argument on civil liberties, Patricia Bellia, a former attorney with the US Department of Justice and an expert in the jurisdictional problems in prosecuting cybercrimes, responds that 'the Convention is not designed to undermine privacy protection', and the Convention's potential for violating fundamental rights has been over-stated.[604] The rights in the Fourth Amendment and other relevant rights will remain as powerful as they were.[605] Secondly, as a response to the obligations of the Internet Service Providers, for the first, the Department of Justice explained that the Convention 'does not contain any mandatory retention provisions or requirements that service providers collect or maintain categories of data generally; nor does it require certain technical capabilities'.[606] The data the Internet Service Providers need to provide if requested in certain circumstances is that already in their possession rather than their retention.[607] For the second, the Department of Justice expressed that the CoC does not require Internet Service Providers to monitor content, nor to be criminally liable if they fail to monitor. Under certain circumstances the Internet Service Providers can be held liable for their employees indeed, while such liability does not go beyond US law governing relevant issues.[608]

After responding to the dissenting opinions, supporters of the CoC also point out that advantages of the CoC outweigh its possible disadvantages. First of all, as an international tool, it unifies nations against cybercrime through furthering the ability of prosecuting cybercrime. For instance, the Convention requires the Signatories to implement minimum

---

[602] See *Frequently Asked Questions and Answers about the Council of Europe Convention on Cybercrime (Draft 24 REV2).*

[603] See Sara L. Marler, 'The Convention on Cybercrime: Should the United States Ratify?' *New England Law Review,* vol. 37 1(2002): 183-219. See also *Frequently Asked Questions and Answers about the Council of Europe Convention on Cybercrime (Draft 24 REV2).*

[604] Robert Lemos, International Cybercrime Treaty Finalized, *CENT News*, 22 June 2001, available at http://news.cnet.com/2100-1001-268894.html. Last visited March 2015.

[605] Sara L. Marler, 'The Convention on Cybercrime: Should the United States Ratify?' *New England Law Review*, vol. 37 1(2002): 183-219, p. 207.

[606] *Frequently Asked Questions and Answers about the Council of Europe Convention on Cybercrime (Draft 24 REV2).*

[607] *Ibid.*

[608] See *Frequently Asked Questions and Answers about the Council of Europe Convention on Cybercrime (Draft 24 REV2).*

substantive cyber offences and enacting procedural laws allowing investigation of computer crimes. Besides, it also establishes international support for investigating and prosecuting computer crimes by setting mutual assistance and international cooperation as obligations.[609] Thirdly, an international treaty like this can help to reduce the finical loss that victims of cybercrime would suffer.[610] As a matter of fact, the losses due to cybercrime are huge, especially when the US government or big businesses become the target of computer crime.[611] A signal that criminal action can and will be prosecuted will help to reduce the crime rate, and thus the consequential loss. To extort such signal, international instruments can help.[612]

4.5 Summary

As a forerunner that uses criminal law to regulate cyber activities, the US promulgated the CFAA as early as 1984. To keep pace with the development of information technology and criminalise new-emerged cyber wrongdoings, the CFAA has been amended eight times, all of which expanded the regulatory scope of the CFAA to a new level. From the term 'federal interest computer' to 'protected computer', the definition of computers covered by the CFAA changed from relatively narrow (only computer used in particular ways) to normal (computers used by federal government or had interstate element[613]), and eventually to broad (almost all common household items and anywhere the computer is in the world[614]). As Judge Easterbrook expressed in the case *US v. Mitra*,

> 'Mitra's problem is not that § 1030 has been turned in a direction that would have surprised reasonable people; it is that a broad statute has been applied *exactly as written* [emphasis added]…There is no constitutional obstacle to enforcing broad but clear statutes.'[615]

---

609 *Ibid*.

610 See Sara L. Marler, 'The Convention on Cybercrime: Should the United States Ratify?' *New England Law Review*, vol. 37 1(2002): 183-219, p. 212.

611 See *ibid*, p. 215.

612 See *ibid*, p. 216.

613 See Michael Hatcher, Jay McDannell and Stacy Ostfeld, 'Computer Crimes', *American Criminal Law Review*, vol. 36 (1999): 397-444, pp. 481-488.

614 See Orin S. Kerr, 'Vagueness Challenges to the Computer Fraud and Abuse Act', *Minnesota Law Review*, vol. 94 (2009): 1561-1587, pp. 1577-1578.

615 *United States v. Mitra*, 405 F.3d 492, 496 (7th Cir. 2005). In this case the defendant used radio hardware and computer equipment to send signals to a communication system. His behaviour prevented the system from receiving essential communications for emergency services. During the trial the prosecution and the defence

This 'broad but clear' approach the US takes on penalising cyber wrongdoings is not without problems. One major concern is its attitude towards computer and data. On hacking offences the legislators choose a narrow perspective and protect the security of the computer; while in other offences such as trafficking in devices, the related sections rely on the concept of data and information. Taking these two perspectives into consideration, people can find the US cybercrime legislation less consistent, and such inconsistency leads to problems in judicial practice. There have been many discussions on whether to incriminate or to criminalise certain behaviour, for instance the recent discussions on how to interpret 'authorisation', and whether an employee is liable for misusing data/information gained from company computers.[616] The issue behind these discussions is in fact which approach is more appropriate: protecting computer or protecting data. Judging from the statutes and academic articles in the US, the legislators and scholars have not reached a consensus on this issue yet.

In the process of amending the CFAA, hardly any room is left for case law. The role of case law in the field of cybercrime legislation is more to clarify meanings of terms rather than to promote far-reaching changes. For many occasions, as illustrated by the cases depicted in this Chapter, judges have noticed the inconsistencies among judgements and thus prefer not to make aggressive and broad interpretations.[617]

Compared with the changes made to the substantive criminal law, new provisions and measures enacted in the procedural criminal law with respect to jurisdiction seem more consistent. The US almost has given itself the jurisdiction over computer misuse around the world. The extra-territorial principle on jurisdiction issue will empower the US judicial organs to investigate, prosecute and adjudicate cyber cases happened over the world unless any of the computers involved is not connected to the Internet. But, understanding it from another perspective, if any of the computer involved is not connected to the Internet, the damage this case may cause will be little, making it less necessary to be incriminated.

---

contested whether the normal function of the system had been impaired by the defendant, in other words, whether the function of a computer was impaired. The defendant was convicted under subsection (a)(5).

[616] For details of this discussion, see e.g. Brandon Darden, 'Definitional Vagueness in the CFAA: Will Cyberbullying Cause the Supreme Court to Intervene?' *Southern Methodist University Science and Technology Law Review*, vol. XIII (2010): 329-358. See also Samantha Jensen, 'Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail', *Hamline Law Review*, vol. 36 (2013): 81-138.

[617] For instance, in the case *United States v. Nosal*, the Ninth Circuit Court of Appeal admitted that 'some courts, including two courts of appeal, have broadly construed the CFAA to hold an employee acting to access an employer's computer to obtain business information with intent to defraud …in violation of the statute', while others have refused to hold employees in the same situation accountable. *United States v. Nosal*, 676 F.3d 854 (9th Cir.2012).

Generally speaking, even though there is no consistent approach or attitude on how to adapt and interpret the CFAA, the US appears remarkably aggressive to combat cybercrime, including the expanding process of the CFAA, the extra-territorial principle of jurisdiction since 1984, and, as being criticised, putting more responsibility on individuals and Internet service providers and granting judicial organs too much enforcement power.[618] Through analysing the arguments behind the offences under the CFAA, it can be observed that the demand for a secure computer and computer network weighs more than the protection of online freedom. This does not mean the US does not protect the individual rights; rather, it means that when balancing online freedom and social interests (including economic interests and national security), the former has been sacrificed to some extent. Such sacrifice, as expressed in a country report of the US, will continue in the future.[619]

[618] Some scholars even suggest that if an actor can store records anywhere in the world through his networked computer, searchers then need an equally broad search warrant to look for the records. But it is debatable whether a judge can execute such a broad warrant without violating the Fourth Amendment's specificity requirement. See Stephen P. Heymann, 'Legislating Computer Crime', *Harvard Journal on Legislation*, vol. 34 (1997): 373-391, pp. 383-385.

[619] The US expressed in its country report for the International Penal Law Association that for future development 'the use of modern telecommunication to contact accused, victims, and witnesses directly over borders should be encouraged', unless the techniques violate the US Constitution or other relative rules. See Bruce Zagaris, International Penal Law Association Report on Information Society, *Section 4, United States Report*, 8 January 2013, available at http://www.penal.org/sites/default/files/files/RH-16.pdf. Last visited March 2015.

Chapter 5 The Cybercrime Legislation in England

5.1 Introduction

This Chapter intends to analyse the legislation on cybercrime in England[620] and unveil the approach behind such legislation. With many people perceiving the existing criminal law in the 1980s as being insufficient or inadequate in cyber context, the legislators enacted the (England) Computer Misuse Act 1990[621] (hereafter the ECMA 1990).[622] Alongside closing the loopholes in the prior law and addressing the issues concerning jurisdiction and extradition, the ECMA 1990 introduces three offences: (1) unauthorised access to computer material, (2) unauthorised access with intent to commit or facilitate commission of further offences, and (3) unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, computer programs and data. In 2001 the United Kingdom signed and the Convention on Cybercrime. To implement the Convention on Cybercrime and to respond to the pressure from the (England) All Party Internet Group (hereafter EAPIG),[623] legislators promulgated the (England) Police and Justice Act 2006[624] (hereafter the EPJA 2006) and amended the ECMA 1990.[625] In 2015, to deter the potential severe damage resulted from unauthorised acts in relation to computer and to meet the requirement of protecting information system of the European Parliament and European Council Directive 2013/40/EU,[626] the (England) Serious Crime Act 2015 (hereafter the ESCA 2015) attaches

[620] England in this thesis is referring to England and Wales. Although the England Computer Misuse Act applies in the Scotland, its application in legal practice is different from that in England and Wales. Thus, Scotland is not discussed in this Chapter.

[621] Computer Misuse Act 1990, available at http://www.legislation.gov.uk/ukpga/1990/18/section/3. Last visited March 2015.

[622] See David Bainbridge, *Introduction to Computer Law* (4th edition), London: Longman, 2000, p. 283.

[623] The All Party Internet Group (APIG) exists to provide a discussion forum between new media industries and Parliamentarians for the mutual benefit of both groups. Accordingly, the group considers Internet issues as they affect society, informing current parliamentary debate through meetings, informal receptions and reports. The group is open to all Parliamentarians from both the House of Commons and the House of Lords. For more details see 'Revision of the Computer Misuse Act-Report of an Inquiry by the All Party Internet Group', June 2004, available at http://www.cl.cam.ac.uk/~rnc1/APIG-report-cma.pdf. Last visited March 2015.

[624] Police and Justice Act 2006.

[625] David Bainbridge, 'Criminal Law Tackles Computer Fraud and Misuse', *Computer Law and Security Report*, vol. 23 (2007): 276-281.

[626] Sections 127 and 128 of the Explanatory Notes of Serious Crime Act 2015, available at http://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/2. Last visited September 2015. See also David Ormerod and Karl Laird, *Smith and Hogan's Criminal Law* (14th edition), Oxford: Oxford University Press, 2015, pp. 1178-1180.

criminal liability to unauthorised acts in relation to computers causing, or creating risk of, severe damage.

5.2 provides a historical review of English cybercrime legislation, intending to reveal the amendments to the ECMA and address the issue how England struck the balance between online freedom and controlling cyberspace in the history. 5.3 presents and explores relevant legislation on computer misuse, generalising the features of the legal system criminalising computer misuse. After investigating the evolution and the current situation of the legislation on cybercrime in England, 5.4 examines the scope of cybercrime in English cybercrime legislation. In the end, 5.5 draws the conclusion of this Chapter, summarising the approach taken in England criminalising computer misuses.

5.2 Historical Review of the Cybercrime Legislation in England

5.2.1 The evolution of Computer Misuse Act

The history of criminalising computer misuses can be divided into three periods: pre 1990, the judges tried to apply traditional criminal provisions to deal with computer crime, and found them inappropriate in cyber context; from 1990 to 2006, after the promulgation of the ECMA, the English legislators and judicial agencies started to apply cybercrime legislation and found the legislation gradually out-dated; the third period is from 2006 to the present day, in which the system of criminalising cyber wrongdoings has been gradually established in England.

5.2.1.1 Pre 1990: initial attempts to use traditional criminal law tackling computer misuses

Before the promulgation of the ECMA 1990, scholars believed that the then 'existing legislation and the common law could deal adequately with the problems thrown up by the use of computers and information technology'.[627] The Law Commission also considered that 'the general criminal law [was] sufficient to deal with most forms of computer misuses'.[628] This opinion was popular up until the end of the 1980s, when in several high-profile cases judges found it hard to stretch the then existing laws ruling certain behaviours.[629] In this period, judges explored traditional criminal provisions from criminal damage to theft and

[627] Andrew Charlesworth, 'Legislating against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990', *Journal of Law and Information Science*, 1(1993): 80-93, p. 81.

[628] The Law Commission, *Computer Misuse working Paper No. 110*, [summary].

[629] Andrew Charlesworth, 'Legislating against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990', *Journal of Law and Information Science*, 1(1993): 80-93.

forgery. However, none of them could appropriately apply to computer misuse without causing more problems. The attempts are as follows.

(1) The first attempt: Criminal Damage Act

At the beginning of the legal fight against computer misuse, traditional criminal provisions could apply to some forms of computer crime. For instance, deleting computer data stored on a disc tended to fall within the scope of section 1(1) of the (England) Criminal Damage Act 1971[630] (hereafter the ECDA 1971).[631] Section 1(1) states that

> 'a person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence'.

However, this provision was insufficient: it only applied when a physical property was destroyed or damaged. It is stated clearly in section 10(1) of the CDA 1971 that 'in this Act, "property" means property of a tangible nature…' Taking the intangible nature of computer data into consideration, the requirement of 'tangible' property in the CDA 1971 limited its use in combating the addition, deletion or damage of computer data stored on a disc.

To apply the CDA 1971 on computer misuses, some expansion had been made when interpreting 'tangible property'.[632] In the case *Cox v. Rilley*, the defendant deleted the data stored on a card and therefore made the card inoperable.[633] He claimed that the damage was made to the data rather than the card, and the card *per se* suffered no impairment, thus the physical property – the card was not damaged. With this argument, he maintained that his behaviour fell outside of the scope of the CDA 1971.[634] Countering such an argument, the Divisional Court rejected it by stating that

---

[630] Criminal Damage Act 1971, available at http://www.legislation.gov.uk/ukpga/1971/48/contents. Last visited March 2015.

[631] Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change', *Journal of Criminal Law*, vol. 70 5 (2006): 424-442, p. 425.

[632] *Ibid*.

[633] *Cox v. Rilley*, [1986] 83 Cr App R 54, DC.

[634] See Martin Wasik, 'Criminal Damage/Criminal Mischief', *Anglo-American Law Review,* vol. 17 (1988): 37-45. See also Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change', *Journal of Criminal Law*, vol. 70 5 (2006): 424-442.

> 'we would not answer the question posed by the justices "can the erasing of a program from a circuit card which is used to operate a computerised saw constitute damage within the meaning of the Criminal Damage Act 1971?" with the emphatic answer yes'.[635]

It can be seen from this statement that the tangibility of the property remained a central issue when ruling such cases. Also with regard to this case, the Law Commission shared a similar opinion with the Divisional Court; it expressed that

> 'the program itself is intangible but, so long as the defendant is charged with causing damage to some tangible part of the computer's hardware on which the information is stored…then, it seems clear, he can be convicted of damage to that hardware if he deletes or alters a program'.[636]

Despite this issue, the CDA seemed to be a potential measure to combat computer crimes in the early stages, supported by the court judgement of the case *Cox v. Rilley* and the Law Commission's position. Some scholars also supported this view. For instance, David Bainbridge concluded in his article that a hacker indeed did not damage the storage media itself, what he did was change the information the media conveyed. This act damaged the integrity of the storage media and thus the actor was guilty of criminal damage.[637]

However, this route, as suggested by Martin Wasik, 'would probably [make] the law undesirably wide merely to include criminal mischief within the simple offence of criminal damage'.[638] Thus, other routes were also explored during that period.

(2) The second attempt: Theft Act

---

[635] Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change', *Journal of Criminal Law*, vol. 70 5 (2006): 424-442, pp. 425-426. Regarding this case, David Bainbridge argued that it was the magnetic impulses that conveyed information rather than the storage media that were damaged in cases as such. See David I. Bainbridge, 'Hacking-The Unauthorised Access of Computer Systems; the Legal Implications', *The Modern Law Review,* vol. 52 (1989): 236-245, pp. 240-241.

[636] The Law Commission, *Computer Misuse working Paper No. 110*, [3.37].

[637] David I. Bainbridge, 'Hacking-The Unauthorised Access of Computer Systems; the Legal Implications', *The Modern Law Review*, vol. 52 (1989): 236-245, p. 241.

[638] Martin Wasik, 'Criminal Damage/Criminal Mischief', *Anglo-American Law Review,* vol. 17 (1988): 37-45, pp. 44-45.

The second possible route was to employ abstraction of electricity - section 13 of the (England) Theft Act 1968[639] (hereafter the ETA 1968) - to regulate computer crimes.[640] This section reads that

> 'a person who dishonestly uses without due authority, or dishonestly causes to be wasted or diverted, any electricity shall on conviction be liable to imprisonment for a term not exceeding five years.'

This offence aims at the acts of bypassing electricity metres, and it seems to have nothing to do with computer misuse. Nonetheless, as argued, a person who uses another's computer without authority will inevitably dishonestly use electricity without due authority, thus resulting in a violation of section 13 of the TA 1968.[641]

No cases were adjudicated based on this section of the TA 1968 in England, but a case which happened in Hong Kong can serve as an example of using this offence to deal with computer misuses.[642] In the Hong Kong case, the defendant discovered a password by coincidence and gained access to a Cable and Wireless plc email system. He confessed that he did this out of curiosity rather than for any kind of personal gain. He was prosecuted and found guilty under section 15 of the Theft Ordinance, which is worded identically to section 13 of the TA 1968.[643]

Though strongly backed by several judges and scholars, applying abstraction of electricity to regulate computer misuse seemed less persuasive to others. For instance, a magistrate commented on the Hong Kong case that no conviction should be imposed to the offender considering the fact that the value of the electricity abstracted had been proved to be around one-eighth of a Hong Kong cent.[644] Similar to his opinion, Martin Wasik argued that considering the value of the electricity used by the offender, such an act was merely a

---

[639] The Theft Act 1968, available at http://www.legislation.gov.uk/ukpga/1968/60/contents. Last visited March 2015.

[640] Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change', *Journal of Criminal Law*, vol. 70 5 (2006): 424-442, pp. 426-428. Section 13 of the Theft Act 1968 outlaws the behavior of 'dishonestly [use] without due authority, or dishonestly [cause] to be wasted or diverted, any electricity'.

[641] *Ibid*.

[642] Hong Kong was a British territory before 1 January 1997.

[643] Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change', *Journal of Criminal Law*, vol. 70 5 (2006): 424-442, p. 426.

[644] *Ibid.*

mischief that differed a lot from misuse, let alone crime.[645] In this regard, section 13 of the TA 1968 is not adequate to apply.

In addition, David Bainbridge expressed his concern over this route, that 'every hacker is committing this offence (abstraction of electricity) regardless of the nature of his actions'.[646] If using this Act, all computer misuses can be tackled under section 13 of the TA. Before reaching this conclusion, Bainbridge argued that

> 'the very act of hacking will result in the host computer (the computer hacked into) performing work…more electricity will be used in transmitting the information to the hacker's computer terminal. The total amount of electricity used to perform these acts will, of course, be tiny but a definite amount will have been used on account of the hacker's act'.[647]

Therefore, the Theft Act route could not adequately apply either.

(3) The third attempt: Forgery and Counterfeiting Act

Since both the CDA 1971 and the TA 1968 had flaws when dealing with crimes involving computers, judges and scholars tried the third route, i.e. to employ the (England) Forgery and Counterfeiting Act 1981 (hereafter the EFCA 1981). However, this route was also proved inadequate. For instance, in the case *R v. Gold and Another,*[648] the limitations of stretching the EFCA to deal with computer hacking were highlighted by the fact that the defendants were found not guilty because of the lack of 'false instrument'.

In this case, by using the users' information and passwords that the defendants had obtained without permission, they hacked into databank, obtained information without paying for it and altered data without authority. Originally, the defendants were convicted under the FCA 1981 section 1(1), which states that

---

[645] Martin Wasik, 'Criminal Damage and the Computerized Saw', *National Law Journal*, vol. 136 (1986), p. 763. Cited in Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change', *Journal of Criminal Law*, vol. 70 5 (2006): 424-442, pp. 426-427.

[646] David I. Bainbridge, 'Hacking-The Unauthorised Access of Computer Systems; the Legal Implications', *The Modern Law Review*, vol. 52 (1989): 236-245, p. 240.

[647] *Ibid*.

[648] *R v. Gold and Another,* [1988] 2 WLR 984, [1988] AC 1063, [1988] 2 All ER 186.

> 'a person is guilty of forgery if he makes a false instrument, with the intention that he or another shall use it to induce somebody to accept it as genuine, and by reason of so accepting it to do or not to do some act to his own or any other person's prejudice'.

In the first instance, the defendants were convicted without heated debate in the court.[649] Nonetheless, when the decision was appealed to the Court of Appeal, arguments were raised about the definition of 'false instrument', which, according to section 8(1), includes: '(a) any document, whether of a formal or informal character; (b) any stamp issued or sold by a postal operator; (c) any Inland Revenue stamp; and (d) any disc, tape, sound track or other device on or in which information is recorded or stored by mechanical, electronic or other means'. Judges in the Court of Appeal held that all of the forms of instrument listed in this provision were tangible; while the electronic impulses generated by typing information and passwords into computer were intangible; therefore, electronic impulses could not constitute false instrument as described in section 8(1), therefore the defendants did not violate section 1.[650]

Opposing this legal reasoning, the public prosecutors argued that at the very point when the defendants typed the customer information and password into the computer, the false instrument was generated, 'with the intent of using it to induce the databank to accept it as genuine to the prejudice of the company operating the system'.[651]

In the next proceeding, the House of Lords, sharing the same opinion with judges in the Court of Appeal, rejected the opinion maintained by public prosecutors and stated that

> 'a device could not be an instrument under section 8(1)(d) of the [FCA] 1981 by which the information was recorded or stored by electronic means, unless it preserved the information for an appreciable time with the object of subsequent retrieval or recovery. Since the momentary holding of the customer identification numbers and passwords while they were verified did not amount to the recording and storage of information, the respondents had not made an instrument within section 8(1)(d) and could not be guilty of an offence under section 1'.[652]

---

[649] Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change', *Journal of Criminal Law*, vol. 70 5 (2006): 424-442, p. 428.

[650] *Ibid*, pp. 428-429.

[651] *Ibid*.

[652] *Ibid*.

In addition, Lord Brandon of Oakbrook also supported the opinion of the Court of Appeal and commented that 'the language of the Act was not intended to apply to the situation which was shown to exist in this case'.[653] Before he concluded this, he suggested that

> 'I share the view of the Court of Appeal (Criminal Division), as expressed by Lord Lane C.J. that there is no reason to regret the failure of what he aptly described as the Procrustean attempt to force the facts of the present case into the language of an Act not designed to fit them'.[654]

This is not the first time he expressed his opinion on 'false instrument'. He once suggested in a report of the Law Commission that

> 'in order to meet the definition of an instrument in section 8(1)(d) of the [FCA] 1981, information must be recorded or stored on or in a disk, tape, soundtrack or other device. To give effect to the everyday meaning of recorded or stored, the information must be held firstly, for an appreciable time and, secondly, with the object of subsequent retrieval or recovery'.[655]

Lord David Brennan as well supported his colleagues in the House of Lords proceedings by stating that

> 'It is a conclusion which we reach without regret. The Procrustean attempt to force these facts into the language of an Act not designed to fit them. This produced grave difficulty for both the judge and the jury which we do not want to see repeated.'[656]

What's more, if the conviction, expressed by Bainbridge, had been upheld, a conclusion would be made that the computer had been deceived, which seems against common sense.[657]

Therefore, all the attempts had been proved either insufficient or inadequate, and other measures were to be tried in the latter stage of combating computer misuses.

---

[653] *R v. Gold and Another,* [1988] 2 WLR 984, [1988] AC 1063, [1988] 2 All ER 186.

[654] *R v. Gold and Another,* [1988] 2 WLR 984, [1988] AC 1063, [1988] 2 All ER 186.

[655] The Law Commission, *Computer Misuse working Paper No. 110*, [3.21].

[656] See *R v. Gold and Schifreen,* [1988] AC 1063. See also Colin Tapper, 'Judicial Attitudes, Aptitudes and Abilities in the Field of High Technology', *Monash University Law Review*, vol. 15 (1989): 219-228.

[657] David I. Bainbridge, 'Hacking-The Unauthorised Access of Computer Systems; the Legal Implications', *The Modern Law Review*, vol. 52 (1989): 236-245, p. 238.

5.2.1.2 From 1990 to 2006: the first legislation on computer misuse

The acquittals of the defendants in the abovementioned case *R v. Gold and Another* dissatisfied the public. As a consequence, they put tremendous pressure on the Law Commission and the legislature. Legal scholars gradually realised that, as Lloyd put it, 'legislative action should not be long delayed'.[658]

In April 1989, a Private Member's Bill concerning criminalising computer misuses was submitted to the Parliament. However, it did not receive much attention. Several months later when the government started to legislate based on the Report of the Law Commission of England and Wales-*Report No. 186, Computer Misuse,*[659] the discussion on criminalising computer misuse was finally initiated. Nonetheless, the government failed to introduce a Bill to integrate and implement all relevant proposals.[660] In the end, following the report of the Law Commission (*Computer Misuse Working Paper No. 110*), another Private Member's Bill was submitted and subsequently became the Computer Misuse Act 1990 after discussions in the Parliament.[661]

This Act, however, became out-dated because it could not cover the new forms of computer misuse, such as the Denial of Service attack. For this reason, a call for amending the ECMA 1990 was raised.

5.2.1.3 After 2006: updates and expansions

With respect to the criticism of the lack of coverage, and as a response to the recommendations for reforms,[662] and to the requirement of the Convention on Cybercrime and the Directive 2013/40/EU, amendments are made to the ECMA 1990 by the EPJA and the ESCA, in 2006 and 2015 respectively.

The EPJA 2006 introduced a new offence of 'making, supplying or obtaining articles for use in offence under section 1 or 3', which states that

---

[658] Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change', *Journal of Criminal Law*, vol. 70 5 (2006): 424-442, p. 429.

[659] The Law Commission, *Criminal Law-Computer Misuse, No. 186(1989).*

[660] Stefan Fafinski, 'Access Denied: Computer Misuse in an Era of Technological Change', *Journal of Criminal Law*, vol. 70 5 (2006): 424-442, p. 429.

[661] Andrew Charlesworth, 'Legislating against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990', *Journal of Law and Information Scienc*e, vol. 4 1(1993): 80-93, p. 82.

[662] 'Revision of the Computer Misuse Act-Report of an Inquiry by the All Party Internet Group', June 2004, available at http://www.cl.cam.ac.uk/~rnc1/APIG-report-cma.pdf. Last visited March 2015.

> '(1) a person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3;
>
> (2) a person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3;
>
> (3) a person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3'.[663]

Admittedly, the primary purpose of the EPJA is to promote policing reforms, thus the change it made to the ECMA 1990 were mainly 'peripheral to the main debate' of cybercrime.[664] However, it is in the discussions on the EPJA 2006 that the concern over cyber terrorism was for the first time officially raised. For instance, Charles Clarke, a Member of Parliament, linked cybercrime with terrorism and serious organised crime to justify the importance of reforming the ECMA. When introducing the Second Reading of the Police and Justice Bill in the House of Commons, he sincerely expressed that

> 'We must recognise that in an increasingly inter-dependent world, work with international partners to tackle terrorism and serious organised crime will be increasingly important. We have therefore included a number of measures to strengthen policing at international level. Computer misuse—the continued threat posed by computer hacking and denial-of-service attacks—is one of the growing new threats that can be tackled only through extensive international co-operation. To that end, the Bill takes up a private Member's Bill tabled by my hon. Friend the Member for Glasgow, South (Mr. Harris) to amend the Computer Misuse Act 1990. I am grateful to my hon. Friend for his initiative.'[665]

Even though in the House of Commons debate on the EPJA 2006 members of Parliament touched upon the new threats to terrorism and national security, the outsiders who voted for

---

[663] Section 3A(1)-(3) of the Computer Misuse Act.

[664] *Ibid,* p. 54.

[665] House of Commons Hansard Debates for 6 Mar 2006, column 618, available at http://www.publications.parliament.uk/pa/cm200506/cmhansrd/vo060306/debtext/60306-09.htm. Last visited March 2015.

tightening laws on computer misuse did not mention such threats; they were discussing the commercial costs of the prevention of hacking.[666] As a response to the same demand from different groups, 'the bill will increase penalties for hacking, viruses and other cyber-crimes to reflect their severity. … In addition we are looking to amend section 3 of the Computer Misuse Act to clarify that all means of interference to a computer system are criminalised,' a Home Office spokeswoman told the media.[667]

The amendments made by the SCA 2015 further illustrate the fact that the concern over cyber terrorism and subsequent damage to national security becomes the main factor that pushes the legislator tightening the law. Fearing that the punishments for offences under sections 1 – 3A of the ECMA are 'too low for the level of economic and personal harm' that cyber attacks on essential systems (such as those controlling power supply and traffic) may cause,[668] and to make ECMA complaint with Directive 2013/40/EU of the European Parliament and European Council,[669] two amendments are made by the ESCA 2015. These two amendments are the introduction of 'unauthorised acts causing, or creating risk of, serious damage', and the extension of section 3A(3) to include an offence of obtaining a tool for use to commit offences under ECMA *regardless of an intention to supply* that tool. In the offence introduced by the ESCA 2015, national security is especially emphasised through attaching a heavier punishment to offences threatening it.[670]

Generally speaking, the ECMA has a limited criminalising scope, and its amendments have not expanded its reach enormously, the reason for the amendments are mainly according to the development of information technology and cybercrime. In this context, the protection of online freedom outweighs the control over cyberspace.

---

[666] Stefan Fafinski, 'Computer Misuse: the Implication of the Police and Justice Act 2006'*, Journal of Criminal Law*, vol. 72(2008): 53-66, p. 55. See also D. Thomas, 'New Bill to Beef up E-crime Law: Home Office Proposes Tougher Sentences for Hackers and Virus Writers', *Computing*, 25 January 2006, available at http://www.computing.co.uk/ctg/news/1848730/new-beef-crime-law. Last visited February 2015. In this piece of news the author estimated that the commercial cost of electronic attacks and denial-of-service attacks for UK business would be over 3 billion euros.

[667] D. Thomas, 'New Bill to Beef up E-crime Law: Home Office Proposes Tougher Sentences for Hackers and Virus Writers', *Computing*, 25 January 2006, available at http://www.computing.co.uk/ctg/news/1848730/new-beef-crime-law. Last visited February 2015.

[668] 'Impact Assessment of Serious Crime Bill: Computer Misuse Act 1990 – Aggravated Offence', 2 June 2014, p. 1, available at http://www.parliament.uk/documents/impact-assessments/IA14-21B.pdf. Last visit September 2015.

[669] Sections 127 and 128 of the Explanatory Notes of Serious Crime Act 2015.

[670] Section 3ZA of the ECMA.

5.2.2 Competing arguments behind the criminalisation of mere hacking

The major considerations expressed during parliamentary discussions on the EPJA 2006 and the ESCA 2015 concerning computer misuse echo the issues discussed regarding the ECMA 1990, namely, the desired scope of the computer-specific law, and the advantages and disadvantages of setting a wide net with respect to computer misuse.[671] When setting this scope, different groups raised different considerations. The discussion around whether to criminalise mere hacking exemplifies these considerations.

5.2.2.1 Arguments for criminalising mere hacking

The first argument is mainly raised by commercial organisations. They maintained that criminalising mere hacking could contribute to the sustainable development of information technology. Acknowledging the importance of computers for the whole society, scholars expressed that computer users tend to fear that others may get access to their personal information stored on their computers, and thus be hesitant in using computers; this may result in the stagnation of information technology.[672] This conjecture worries the commercial organisations, and they subsequently maintained that to prevent this from happening, mere hacking should be criminalised.

The second justification rests on the fundamental role that computers play in the functioning of society. Computers had become part of the national infrastructure, vital to commerce, communication, security and welfare. The damage might arise even if the hacker only obtained access and caused no impairment to the data, to be specific, the 'risk of inadvertently damaging or destroying data files or programs and thereby disrupting the works in progresses'.[673] In addition, information the hacker obtained after the mere hacking presented the risk of further consequences, such as the disclosure of classified information. These

[671] See Lords Hansrd text for 11 July 2006, Debate on Police and Justice Bill, available at http://www.publications.parliament.uk/pa/ld199697/ldhansrd/pdvn/lds06/text/60711-0003.htm#06071147000006. Last visited March 2015. See also House of Commons Hansard Debates for 6 Mar 2006, colomn 618, available at http://www.publications.parliament.uk/pa/cm200506/cmhansrd/vo060306/debtext/60306-09.htm. Last visited March 2015.

[672] The Law Commission, *Computer Misuse working Paper No. 110*, [6.8]. See also, Home Office, *Cyber Crime Strategy cm 7842*, UK: The Stationery Office Limited, 2010, [8].

[673] The Law Commission, *Computer Misuse working Paper No. 110*, [6.9]-[6.12].

scenarios pushed the government and the legislature to take measures, including criminalising mere hacking.[674]

The third argument is raised from the perspective of the deterrence function of the criminal law. Those who hold this idea claimed that the society 'must try to deter hacking either generally, or at the very least in respect of computers holding certain kinds of information'.[675] Even, as some scholars worried, that an offence like mere hacking would incur relatively low punishment and thus most of them would be solved before getting to court, the introduction of such an offence 'would signal society's disapproval of those who deliberately set out to breach security measures, and amount to a rejection of the claim that hacking is a harmless intellectual pastime'.[676]

The fourth argument is based on the criminalisation of mere hacking in other jurisdictions. Before the creation of an offence for obtaining unauthorised access to a computer, the Scottish Law Commission recommended criminalising such conduct. Furthermore, other commonwealth countries such as Canada and many states in the US have also chosen to enact criminal offences concerning unauthorised access to computers or data.[677] Their choice suggests the necessity of criminalising mere hacking.

5.2.2.2 Arguments against criminalising mere hacking

The primary argument against an offence as mere hacking is that although such conduct may infringe privacy, it is not harmful or serious enough to launch a criminal procedure. Since privacy was not explicitly protected by laws in England until the promulgation of the Data Protection Act 1998, obtaining unauthorised access to personal data would not constitute a criminal offence unless a further crime was committed or attempted. At that time, the English legal system did not recognise data as the subject of laws, so obtaining and reading others' information constituted no offence.[678] This argument, however, was over-turned by the Data Protection Act 1998.

---

[674] Jonathan Clough, 'Data Theft? Cybercrime and the Increasing Criminalization of Access to Data', *Criminal Law Forum*, vol. 22(2011): 145-170, pp. 159-161.

[675] *Ibid*, pp. 159-162.

[676] The Law Commission, *Computer Misuse working Paper No. 110*, [6.12]. See also Home Office, *Cyber Crime Strategy cm 7842*, UK: The Stationery Office Limited, 2010, [18].

[677] The Law Commission, *Computer Misuse working Paper No. 110*, [6.13]-[6.14].

[678] The Law Commission, *Computer Misuse working Paper No. 110*, [6.15].

The second reason for rejecting the creation of an offence as mere hacking relies on the enforcement measures of similar offences. It has long been recognised that there was a significant possibility that mere hacking would remain unnoticed. Besides, even if such conduct were reported, the investigation would be too complicated and time-consuming to achieve. Because such conduct could mostly be discovered after data had been erased or altered, or after a further offence had been attempted, 'a charge of criminal damage or an offence of fraud may then be the appropriate response'. In this regard, a special criminal provision on obtaining unauthorised access to data hardly seemed necessary.[679]

In the computer misuse working paper No. 110 published by the Law Commission, a recommendation was put forward that no special provisions should be made for less serious offences.[680] Before proposing this recommendation, they maintained that criminal liability should not exist just because a computer was involved. Otherwise, the English law in this field would become 'undesirably wide and uncertain'.[681] However, this proposal was rejected by the legislature, as section 1 of the ECMA shows, under which mere hacking is criminalised.

5.3 Current Legislation on Cybercrime

The ECMA 1990 sets the structure of cybercrime legislation, and the EPJA 2006 and the SCA 2015 make several adjustments to it in order to match the development in cybercrime. These three Acts constitute the cybercrime legislation system in England.

5.3.1 Offences against the security of computer

Adopting the framework of offences introduced in the Convention on Cybercrime of the Council of Europe, offences under this category include access offences (i.e. hacking), impairment of data, interception of data, and misuse of devices, as well as the one introduced in 2015: unauthorised acts causing severe damage.

---

[679] The Law Commission, *Computer Misuse working Paper No. 110*, [6.16].

[680] The Law Commission, *Computer Misuse working Paper No. 110*, [8.3]-[8.11]. See also Martin Wasik, 'Computer Misuse: the Law Commission's Working Paper on Computer Misuse', *The Computer Law and Security Report*, 5(1989): 2-4.

[681] Martin Wasik, 'Criminal Damage/Criminal Mischief', *Anglo-American Law Review*, vol. 17 (1988): 37-45.

5.3.1.1 Access offences

Section 1 and 2 of the ECMA penalises hacking, including unauthorised access to computer materials with and without intent to commit further offences. The analysis of these two offences is conducted under four elements, including computer, access, authorisation, and fault element.

(1) Computer

Although section 1 and section 2 are entitled 'unauthorised access to computer material', the term 'computer' remains undefined in English criminal law. It was a specific decision made by the legislators, following the recommendation of the Law Commission. The debate behind this decision is discussed in 5.4 the scope of cybercrime.

Analysing sections 1 and 2 one can notice that in England it is the data stored on a computer, rather than the computer itself that is protected by the cybercrime legislation. Taking section 1 as an example. Securing access to any program of data held in any particular computer constitutes a crime. The 'program or data held in any particular computer', as explained in section 17(6) of the ECMA, refers to 'any program or data held in any removable storage medium which is for the time being in a computer, and a computer is to be regarded as containing any program or data held in any such medium'.[682] Under this explanation, it can be concluded that securing access to data will inevitably cause computer to respond to some extent. The security of computer and data thus seem to be the same. It is true? Data contains information, and it is therefore protected, especially its confidentiality. Mere hacking to data damages the confidentiality of data, thus it is criminalised. In this sense, the computer is just a physical container for data.[683] As Clough suggests, 'what is punished is in fact unauthorised access to computer data, rather than the computer itself.'[684]

Taking one step further, this rationale of protecting data also relates to the discussion on whether 'data' belongs to 'property' discussed before the promulgation of the ECMA, and, even to the relationship between traditional criminal law and cybercrime legislation. If, the judgement in the case of *Cox v. Rilley* is taken into consideration, 'property' must be tangible

[682] See section 17(6) of the Computer Misuse Act 1990.

[683] Orin S. Kerr, 'The Problem of Perspective in Internet Law', *Georgetown Law Journal*, vol. 91 11(2002): 357-406, pp. 359-361.

[684] Jonathan Clough, 'Data Theft? Cybercrime and the Increasing Criminalization of Access to Data', *Criminal Law Forum*, vol. 22 (2011): 145-170, p. 157.

and physical, thus a computer and hardware in a computer are property, and data is not. Therefore, if one obtains access to a computer, this computer itself suffers no damage and no traditional provisions apply to this scenario. As the Law Commission maintains, 'if it is not a crime to use someone else's lawnmower without their permission, so long as it is returned undamaged. By analogy, it is not an offence to make unauthorised use of a computer.'[685] Then, one question subsequently emerges: mere hacking does not damage computer, why is it criminalised under the ECMA? It can thus be concluded that it is the damage to data that is prohibited in the ECMA. To be clearer, mere hacking changes the data or program held in the computer since the actor must have caused the computer to function or respond through mere hacking, and cause the data suffering damage, deletion or addition. If the ECMA protects computer only, apparently section 1 should not be drafted. It is thus clear that section 1 protects data, rather than computer. Same rationale applies to section 2. It is also clear that the difference between the ECMA and the traditional criminal law is that the former protects the intangibles, and the latter protects the tangibles.

(2) Access

The term 'access' is interpreted in a broad way in England. Namely, it refers to acts causing 'a computer to perform any function with intent to secure access to any program or data held in any computer'.[686] In fact, the Law Commission rejected the wording 'gain access to computer system or data' used in the Convention on Cybercrime and its Explanatory Report and chose the phrase 'causes a computer to perform any function'. The reasons for this choice, as listed by Jonathan Clough, are as follows:

> 'firstly, [any definition] may be thought to encompass obtaining physical access to a computer; secondly, it could be thought to extend to obtaining a hard copy of data stored in a computer; thirdly, it was felt that such an offence might apply to electronic eavesdropping and thereby go beyond protecting the integrity of computers to protecting the confidentiality of data'.[687]

Disagreeing with the Law Commission's choice and Jonathan Clough's explanation, Martin Wasik argued that the interpretation adopted by England is too broad, so that simply

---

[685] The Law Commission, *Computer Misuse working Paper No. 110*, [1.5].

[686] Section 17(6) of the Computer Misuse Act.

[687] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, pp. 62-63.

switching on a computer or attempting to enter a password without authority would fall within the scope of this expression.[688]

(3) Authorisation

In the legal context of England, access is unauthorised if (a) the person is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled (section 17(5)).

(4) Fault element

Under section 1, an intention to secure access (to any program or data held in any computer, or to enable any such access to be secured) and the knowledge of such access is unauthorised constitute the *mens rea* of this offence. In other words, it is not necessary that the access to a computer must be for fraudulent or other malicious purposes.[689] In addition, the offence under section 1 is accomplished at the very point when the offender intends to and tries to secure access, so prosecutors do not need to prove that the intended access has been achieved.[690]

If unauthorised access is conducted to commit or facilitate further offences, section 2(1) applies.[691] It is immaterial for the purposes of section 2 whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion (section 2(3)), just as it is immaterial for whether the commission of the further offence is possible or not (section 2(4)). As suggested by the Law Commission, this offence 'particularly aim[s] at those cases where the conduct is engaged in with the intention of committing a further offence, in circumstances where the conduct is not sufficiently proximate to the completed offence to constitute an attempt'.[692]

---

[688] Martin Wasik, *Crime and the Computer*, New York: Oxford University Press, 1991, pp. 91-92.

[689] According to section 1(2) of Computer Misuse Act, the intent of the offender can be (a) any particular program or data; (b) a program or data of any particular kind; or (c) a program or data held in any particular computer.

[690] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, pp. 49-50.

[691] In fact, the Law Commission recommended that if there was no further intention to commit other crimes when securing access, there was no criminal offence. This recommendation was not acceptted by the legislators. See Tan Limin and M. Newman, 'Computer Misuse and the Law', *International Journal of Information Management*, 11(1991): 282-291, pp. 283-284.

[692] The Law Commission, *Computer Misuse working Paper No. 110*, [3.50]-[3.53].

5.3.1.2 Impairment of data

Section 3 of the ECMA, substituted by the EPJA 2006, rules that a person is guilty if he does any unauthorised act in relation to a computer, and at the time when he does the act he knows that it is unauthorised (section 3(1)). It must be proven that by conducting such offence he either intends to, or is reckless to whether the act will (a) impair the operation of any computer; (b) prevent or hinder access to any program or data held in any computer; (c) impair the operation of any such program or the reliability of any such data; or (d) enable any of the things mentioned in paragraphs (a) to (c) above to be done (section 3(2)).

Initially, section 3 of the ECMA 1990 was introduced to criminalise the unauthorised modification of contents of computer, including 'erasing or altering data, distributing malware and adding a password without authorisation to restrict access to a file',[693] as to impair the operation of a computer or program or the reliability of data.[694]

Some scholars suggest that an offence under section 3 can also damage a computer physically, and thus it falls within the scope of the Criminal Damage Act 1971 as well.[695] To address this issue, the Law Commission put forward their opinion that, considering the purpose of the Criminal Damage Act 1971, a modification to the computer system or the data stored on a disk 'shall not be regarded as damaging any computer or computer storage medium unless its effect on that the computer or computer storage medium impairs its physical condition'.[696]

Apart from the potential overlap with the CDA 1971, the phrase 'impair the reliability of data' remained unclear. For instance, in the case *Zezev and Yarimaka v. Governor of HM Prison Brixton and another,*[697] the defendant claimed that section 3 did not apply to his case because he did not delete the data but changed it, and his act only impaired the reliability of data, not the computer. He claimed that:

> 'section 3 is confined to those who damage the computer so that it does not record information that is fed into it. If information is accurately fed into the computer but the information is untrue, that does not impair the operation of the computer because

[693] The Law Commission, *Computer Misuse No. 186* (1989), [3.65].

[694] Section 3 of the Computer Misuse Act 1990.

[695] See B. J. George Jr., 'Contemporary Legislation Governing Computer Crimes', *Criminal Law Bulletin*, vol. 21 5(1985): 389-412.

[696] The Law Commission, *Computer Misuse No. 186* (1989), [3.78].

[697] *Zezev and Yarimaka v. Governor of HM Prison Brixton and another*, [2002] 2 Cr App R 33.

> it is meant to record the information as inputted and has done so. Nor is anyone prevented or hindered from accessing that data'.[698]

Lord Chief Justice Woolf, however, rejected this argument. He expressed that

> 'if an individual, by misusing or bypassing any relevant password, places in the files of the computer a bogus e-mail by pretending that the password holder is the author when he is not, then such an addition to such data is plainly unauthorised, as defined in section 17(8); the intent to modify the contents of the computer as defined in section 3(2) is self-evident and, by so doing, the reliability of the data in the computer is impaired within the meaning of section 3(2)(c)'.[699]

Reading this interpretation together with the legislative appraoch (i.e. focusing on data) behind the ECMA, one issue emerges: the threshold of 'impairing' the reliability of data or the operation of programs is uncertain. A crime would be committed and completed as long as the data or program has been added, deleted, modified, and suppressed, in one word, impaired.

The court further extended the ambit of this offence by holding the DoS attack[700] accountable, as the case *R v. Lennon*[701] shows. In fact, the new phenomenon of DoS attack had led to a debate on whether such activity is covered under section 3. In reaction to this debate, the APIG suggested enacting a new offence of impairing access to data.[702] The application of section 3 in the case *R v. Lennon* reflects the judges' rejection of the APIG's proposal and preference on broadening the *actus reus* of section 3.

The interpretation above is obviously broad. Therefore, the problematic section 3 was replaced with a new one. Under the new section 3, all forms of DoS attacks are incriminated,

---

[698] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 116.

[699] *Zezev and Yarimaka v. Governor of HM Prison Brixton and another*, [2002] 2 Cr App R 33.

[700] DoS attack is defined as 'a malicious attempt to disrupt the operation of a specific computer, network, web site or other entity in cyber space'. See Home Office, *Cyber Crime Strategy cm 7842*, UK: The Stationery Office Limited, 2010. DoS attack has several forms, such as sending millions of spams to a server of a company, to prevent 'legitimate' users from obtaining access to or using Internet service. See Kit Burden and Creole Palmer, 'Internet Crime: Cyber Crime – A New Breed of Criminal?' *Computer Law and Security Report*, vol. 19 3(2003): 222-227, p. 223.

[701] *R v. Lennon*, [2006] EWHC 1201. In this case the offender sent huge amount of emails to his former employer's computer and thus choked the computer with rubbish, making it unable to function. The court ruled that section 3 of the ECMA applied to this case.

[702] 'Revision of the Computer Misuse Act-Report of an Inquiry by the All Party Internet Group', June 2004, [56] - [75].

irrespective of whether an attack as such modifies data or not. The term 'unauthorised act' expressly shows that it does not make sense anymore to prove that there is an unauthorised modification of data, and a mere unauthorised act 'in relation to a computer' is enough for incrimination.[703] However, Kit Burden and Creole Palmer criticised such an extensive legislation. They argued that the offenders did not gain access to the target system or modify it in certain forms of DoS attack, thus the ECMA should not cover such acts.[704] For instance, the actor may impair a computer through sending a large quantity of emails to the targeted network server. Under such occasions, the actor does not intend to hack the computer at all, let alone be punished under the ECMA.[705] Burden and Creole are partly right. Their argument only holds true for the old ECMA, which protects data rather than computer. The newly introduced section 3, as its wording indicates, protects not the reliability of data, but the computer. Therefore, the actor does not hack the computer defectively, but he damaged the computer, which under the new section 3 shall be punished. This new section 3, as rightly pointed out by Professor Ian Walden, 'shifts the locus of the crime from the "contents of the computer", to potentially any point in a network which is held to be "in relation to" the target computer.'[706] It is thus clear that the approach of sections 1 and 2 is different from that of the new section 3: the former focuses on data while the latter focuses on computer. Nonetheless, Burden and Creole are partly right because the term 'in relation to computer' is left undefined, which can be interpreted dramatically broad if judges would like to. This phenomenon presents an enormous potential of controlling cyberspace strictly and infringing online freedom.

5.3.1.3 Interception of data

In England, interception of data is criminalised under the (England) Regulation of Investigatory Powers Act 2000 (hereafter the ERIPA 2000), which aims at 'offering a single legal regulatory system' for interception of communications and 'recognising and regulating

[703] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, pp. 107-108.

[704] Kit Burden and Creole Palmer, 'Internet Crime: Cyber Crime – A New Breed of Criminal?' *Computer Law and Security Report*, vol. 19 3(2003): 222-227, p. 223.

[705] *Ibid.*

[706] Ian Walden, 'Computer Crime', *Computer Law*, (2003): 295-329.

the impetus towards state surveillance in the information age'.[707] Namely, section 1(1) and (2) of the ERIPA 2000 makes it an offence for:

> '(1)…a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of -
>
> a public postal service; or
>
> a public telecommunication system.' Or
>
> '(2) by means of a private telecommunication system'.[708]

The ERIPA 2000 puts much stress on distinguishing between a 'public telecommunication system' and a 'private telecommunication system'. A 'public telecommunication system' refers to a system

> '(a)…attached, directly or indirectly and whether or not for the purposes of the communication in question, to a public telecommunication system; and
>
> (b) there is apparatus comprised in the system which is both located in the United Kingdom and used (with or without other apparatus) for making the attachment to the public telecommunication system'.[709]

A private one means any system, 'without itself being a public telecommunication system'.

The reason for separating public and private telecommunication systems is that the defences applying to them are different. For instance, the defence provided by section 1(6) of the ERIPA 2000, that a person has 'a right to control the operation or the use of the system' or 'has the express or implied consent of such a person to make the interception', can only apply to a situation where the interception was made by means of a private telecommunication system.[710]

---

[707] See Y. Akdeniz, N. Taylor and C. Walker, 'Regulation of Investigatory Powers Act 2000 (1): BigBrother. Gov. UK: State Surveillance in the Age of Information and Rights', *Criminal Law Review*, 2(2001): 73-90.

[708] Sections 1(1) and (2) of the Regulation of Investigatory Powers Act 2000.

[709] Section 2(1) of the Regulation of Investigatory Powers Act 2000.

[710] Section 1(6) of the Regulation of Investigatory Powers Act 2000.

In addition, the definition of public communication indicates that an entirely stand-alone system or device that is not connected to a computer network falls out of the range of the ERIPA 2000. In this sense, this section presumably may not cover intercepted communications via Bluetooth or other similar systems either,[711] if Bluetooth is not interpreted as a kind of network. This gap in the law may mean that mobile phones and tablet PCs suffering from hacking by means of a Bluetooth system do not fall under this Act.

As for the term 'communication', in the case *Morgans v. DPP*[712] the judges were confronted by the issue of whether the information obtained through a logging device was a 'communication'. They ruled in their decision that the information obtained was merely 'the time and date on which calls were made, the duration of the calls and the numbers dialled' and thus was not 'communication'.[713] In deciding this case, the court cited the definition of 'communication' used by Lord Oliver in the case *R v. Effik*:[714]

> 'communication … refers to the telephonic communication which is intercepted in fact, and on the evidence…consists of what has been variously described as the electrical impulse or signal which is affected by the interception that is made.'[715]

Based on this definition, Lord Hope, one of the judges of the case *R v. Effik*, stated that

> 'it is sufficient, to constitute a communication by means of a public telecommunication system for the purpose of the Act [the Interception of Communications Act 1985], for an electrical impulse or signal to be transmitted from the telephone number from which the impulse or signal is sent to the telephone number with which it has been connected. The sending of an electrical impulse or signal in either direction will do, irrespective of the response which it elicits from the recipient and the length or content of the message which it conveys'.[716]

---

[711] See Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 149.

[712] *Morgans v. DPP*, [2000] UKHL 9, [2000] 2 All ER 522, [2000] 2 WLR 386, [2000] Crim LR 576, [2001] 1 AC 315, available at http://swarb.co.uk/morgans-v-director-of-public-prosecutions-hl-18-feb-2000/. Last visited March 2015.

[713] *Morgans v. DPP*, [2000] UKHL 9, [2000] 2 All ER 522, [2000] 2 WLR 386, [2000] Crim LR 576, [2001] 1 AC 315.

[714] *R v. Effik,* [1995] AC 1309, available at http://swarb.co.uk/regina-v-effik-regina-v-mitchell-hl-22-jul-1994/. Last visited March 2015.

[715] *R v. Effik,* [1995] AC 1309.

[716] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, pp. 158-159.

It can be seen from this statement that metring information such as that records the date, duration of calls and the number dialled does not count as communication. In accordance with this, the ERIPA 2000 rules that the interception of a communication refers to 'any conduct that takes place in relation only to so much of the communication as consists in any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted'.[717] Therefore, the 'communication' for the purpose of the ERIPA 2000, incorporates only content, not metring information.

With respect to the meaning of 'interception', section 2(2) prescribes that 'a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he (a) so modifies or interferes with the system, or its operation, (b) so monitors transmissions made by means of the system, or (c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication'.[718] Based on this provision, the court has ruled that interception 'denotes some interference or abstraction of the signal, whether it is passing along wires or by wireless telegraphy'.[719] Through interpreting 'interception' like this, England makes its position clear that any change or abstraction of a signal is criminalised.

5.3.1.4 Misuse of devices

As a part of the responsibility to implement the Convention on Cybercrime at the national level, a new section 3A is inserted into the ECMA by the EPJA 2006. Even though the Home Office claimed in 2004 that it was 'unlikely' to criminalise the possession of 'hacking tools' by a new section, the EPJA 2006 demonstrated a different position on this issue. The new section 3A contains three new offences, mainly regarding making, adapting, supplying, offering to supply or obtaining any tool with the ulterior intention of committing offences prescribed in section 1, section 3 (or section 3ZA that inserted in 2015).[720]

[717] Section 2(5) of the Regulation of Investigatory Powers Act 2000.

[718] Section 2(2) of the Regulation of Investigatory Powers Act 2000.

[719] *R v. E,* [2004] EWCA Crim 1243 at [20] per Hughes J.

[720] Section 3A(1)-(3) of the Computer Misuse Act.

The term 'article' used in each of the offence 'includes any program or data held in electronic form'.[721] The word 'includes' indicates that 'article' is not limited to the intangibles. As some scholars suggest, by defining 'article' as such, it definitely includes the intangibles such as malware and passwords.[722] Moreover, it also encompasses the tangibles: 'a computer itself is an article that may be used to commit an offence under section 1 or 3'.[723]

Under section 3A(1), 'supply' or 'offer to supply' would include disseminating articles as well as advertising the supply of such articles.[724] It is immaterial whether such articles can in fact be used in committing offences or not.[725] As an example, providing an incorrect password may still fall within the scope of section 3A, even though such an article is useless, if the required fault element is met.[726]

Section 3A(2) criminalises behaviours that 'supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of' offences under the ECMA. The main issue concerning this offence relates to the dual-use devices. The initially drafted section 3A(b) (i.e. section 3A(2) in the Police and Justice Bill *(draft)*) incurred criticism from the software industry because of the fear that it 'could effectively criminalise IT professionals who use penetration testing - also known as ethical hacking - to identify security weaknesses'.[727] Suppliers of legitimate products such as penetration test software

---

[721] Sections 3A(4) of the Computer Misuse Act.

[722] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 128.

[723] *Ibid*.

[724] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, pp. 128-129.

[725] Section 3A(1) of the computer Misuse Act.

[726] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 129.

[727] W. Goodwin, 'Computer Misuse Act Amendment Could Criminalize Tools Used by IT professionals', 21 February 2006, *Computer Weekly*, available at http://www.computerweekly.com/news/2240076599/Computer-Misuse-Act-amendment-could-criminalise-tools-used-by-IT-professionals. Last visited March 2015.

Section 3A(a) and (b) were phrased as

'a person is guilty of an offence if he makes, adapts, supplies or offers to supply any article—

knowing that it is designed or adapted for use in the course of or in connection with an offence under section 1 or 3; or

intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3'.

In the Commons Committee Stage Lynne Featherstone, Member of Parliament, proposed to change the 'or' to 'and' in the end of subsection (a) to ensure 'that an offence [was] committed only when there [was] possession and intent to use the programs for the purposes of hacking, and so a security consultant using them legitimately to check that a system [was] secure would not be caught by the drafting'. However, this proposal was rejected, and the wording of 'it is likely to be used' was adopted in the final version of section 3A.

were afraid that their products might be used to commit or facilitate an offence and thus expose them to criminal liability.[728] This fear was aggravated by the courts' opinion in the case of *DPP v. Lennon*[729] where judges made no distinction between malicious conduct and conduct on the basis of good intention.[730]

Therefore, in the final version of this subsection, the responsibility of deciding whether an article is likely to be used to commit an offence is imposed to the manufacturers and suppliers. To avoid criminal punishment, they must check carefully whether they are supplying to users who have good intentions. However, this measure would still be problematic since it is hard for suppliers to be confident 'that the purchaser's intentions [are] honourable'.[731] Therefore, the suppliers are hesitating to produce the dual-use tools, and these tools are for great possibility prohibited.

5.3.1.5 Unauthorised acts causing, or creating risk of, serious damage

This offence prohibits the cyber offences that cause serious damage, such as the loss of human life and disruption of the supply of water and electricity. The prohibited acts under this offence, as argued in its Impact Assessment Report, are already covered by section 3; and making it a different and complete offence is to attach heavier punishments to cyber offences causing serious consequences.[732] One issue with respect to its *actus reas* is that it adopts the wording of section 3: unauthorised acts in relation to computer. Although such a wording has appeared in the EPJA 2006, what constitutes 'in relation to computer' is still left untouched, neither in the Explanatory Notes of the Serious Crime Act 2015 nor in the Parliament debate. Moreover, there is less attention even from the academia on this very issue. Thus, many questions are unaddressed, such as why does England use such a broad term 'in relation to'. In addition, as suggests previously, before the EPJA 2006 the ECMA focuses on data, while after it computer starts to get attention. Why does England change its approach? What are the

---

See e.g. Stefan Fafinski, 'Computer misuse: The implications of the Police and Justice Act 2006', *Journal of Criminal Law*, 1(2008): 53-66.

728 Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 129.

729 *DPP v. Lennon*, [2006] EWHC 1201 (Admin), available at http://swarb.co.uk/director-of-public-prosecutions-v-lennon-admn-11-may-2006/. Last visited March 2015.

730 *Ibid*.

731 Stefan Fafinski, 'Computer misuse: The implications of the Police and Justice Act 2006', *Journal of Criminal Law*, 1(2008): 53-66, pp. 63-64.

732 'Impact Assessment of Serious Crime Bill: Computer Misuse Act 1990 – Aggravated Offence', 2 June 2014, available at http://www.parliament.uk/documents/impact-assessments/IA14-21B.pdf. Last visit September 2015.

considerations behind? Does England realise data is no longer the only target of computer crime? Or does England feel incapable of forecasting the future change of cybercrime, and thus make a very broad offence? All of these questions remain unexplained.

5.3.2 Traditional crimes facilitated by computer

Similar to the discussions in the Chapter on the Council of Europe and the Chapter on the US, the offences under 5.3.2 include computer facilitated fraud and forgery, computer facilitated child-pornography crime and computer facilitated copyright related crime.

5.3.2.1 Computer facilitated fraud and forgery

By defining computer fraud as the 'conduct which involves the manipulation of a computer, by whatever method, in order to dishonestly obtain money, property or some other advantage of value, or to cause loss', the Law Commission suggested in its working paper that it would be better to use traditional criminal provisions to deal with computer facilitated fraud since it belongs to fraud.[733] In accordance with this recommendation, computer-related fraud has been dealt with alongside traditional fraud offences in England, namely, through the (England) Fraud Act 2006 (hereafter the EFA 2006), and so have offences like computer related forgery.

In England computer fraud contains two groups: one is the so-called 'real' computer fraud - the ones that involve the dishonest alteration of a computer program, and the other one is using computer as a tool to commit fraud.[734] Although the 'real' computer fraud did not happen as often as the legislators thought, the issue that whether a machine can be deceived is especially addressed.[735]

To be specific, the essence of fraud is that the victim is persuaded to believe that 'a [representation] is true which is false, and which the person practising the deceit knows or believes to be false'.[736] However, in computer related fraud, this is not always the case. For instance, in a typical computer fraud case, the offender intercepts data that he is not authorised to, and obtains some property by using the data he intercepted. In such a case data is normally a PIN code for a card at an ATM or a credit card number that can be used for

[733] Martin Wasik, 'Computer Misuse: the Law Commission's Working Paper on Computer Misuse', *The Computer Law and Security Report*, 5(1989): 2-4, p. 2.

[734] The Law Commission, *Computer Misuse working Paper No. 110*, [2.8].

[735] *Ibid.*

[736] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 204.

online shopping. When receiving the data, the machine starts to 'process the number, check its validity and approve the request'.[737] Considering the essence of fraud, does it hold true that the machine/computer is deceived? In other words, does the computer have the capability of being deceived?

The Law Commission suggests not. It holds the idea that since the machines do not have beliefs and they simply respond to the information that is provided to them, they cannot be deceived.[738] In accordance with this opinion, the EFA 2006 regards a representation as having been 'made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention)'.[739] This explanation suggests that the legislature agrees with the Law Commission and believes a system or a device cannot be deceived: it can only respond to instructions. Moreover, by legislating like this, England avoids answering the question that who is deceived. Rather, as long as a false representation is made to a machine and causes it to respond, a fraud is committed.

5.3.2.2 Offences related to child-pornography

Computer crimes relating to child pornography include producing, possessing, distributing, showing and advertising indecent pornographic material made through exploiting children with the help of computer and/or computer network.[740] Traditionally, England criminalises the 'distribution, showing and advertisement of such indecent photographs',[741] and mere possession of such indecent materials was not an offence. This situation lasted until 11 January 2001, when the Criminal Justice and Court Services Act 2000[742] substituted section 160 into the Criminal Justice Act 1988, according to which possessing indecent photographs is penalised.

In the cyber context, a photograph, stated by the Protection of Children Act 1978, includes 'data stored on a computer disc or by other electronic means which is capable of conversion

[737] *Ibid.*

[738] Law Commission, Fraud- Report on a Reference under Section 3(1)(e) of the Law Commissions Act 1965 *(Law Com. No. 276)*, July 2002, pp. 20-21.

[739] Section 2(5) of the Fraud Act 2006.

[740] Section 1(1) of the Protection of Children Act 1978.

[741] *Ibid.*

[742] See section 41(3) of the Criminal Justice and Court Services Act 2000.

into a photograph'.[743] 'Child' in these offences refers to a person under sixteen. In addition, in accordance with the Convention on Cybercrime, if a person is shown as a child in a 'pseudo-photograph', this pseudo-photograph shall be treated for all purposes as showing a child, and so shall a pseudo-photograph in which 'the predominant impression conveyed is that the person shown is a child notwithstanding some of the physical characteristics shown are those of an adult'.[744]

5.3.2.3 Offences related to infringemtnd of copyright and related rights

In England, the principal legal instrument that applies to copyright crime facilitated by computer is the (England) Copyright, Designs and Patents Act 1988[745] (hereafter the ECDPA 1988). In many circumstances, infringements of copyright have a civil nature, for instance, a copyright owner can bring a lawsuit to the court when, following a breach of his rights under copyright, he suffers damage.[746] Criminal liability can also be pursued regarding copyright violations in England. According to Jonathan Clough, there are four elements separating criminal offences from civil infringements: (1) commercial in nature, (2) distribution, (3) *mens rea* of 'knows or has reason to believe' such article is 'an infringing copy of a copyright work',[747] and (4) significant penalties.[748]

With regard to the first element, the 1988 ECDPA rules that a person commits a criminal offence only when the act is conducted 'in a course of business' or when the actor 'imports into the UK otherwise than for his private and domestic use'.[749] In addition, in situations where the infringement is not in the course of business, a distribution 'to such an extent as to affect prejudicially the owner of the copyright' will also be a criminal offence.[750]

[743] See section 7(4) of the Protection of Children Act 1978.

[744] See section 7(8) of the Protection of Children Act 1978.

[745] The Copyright, Designs and Patents Act 1988, available at http://www.legislation.gov.uk/ukpga/1988/48/contents. Last visited March 2015.

[746] Section 96 of the Copyright, Designs and Patents Act 1988.

[747] Section 107 of the Copyright, Designs and Patents Act 1988.

[748] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, pp. 226-227.

[749] Section 107(1) of the Copyright, Designs and Patents Act 1988.

[750] Section 107(1)(e) of the Copyright, Designs and Patents Act 1988.

5.3.3 Jurisdiction

The ECMA adopts territory jurisdiction and personality jurisdiction. The territory jurisdiction means that when an offence occurred in the home country concerned or the accused was in the home country concerned at the time of the act or event, England has jurisdiction.[751] By saying 'home country', the legislators refer to England and Wales, Scotland, and Northern Ireland.[752] The personality jurisdiction is also attached to cybercrime. It means if the accused is a UK national at the time the offence was committed, and the act in question also constitutes a crime according to the law of the country the act occurred, England has jurisdiction.[753]

However, the ECMA in fact has the extra-territorial jurisdiction. When preparing the ECMA 1990, the Law Commission raised several issues regarding the principle that should be adopted for the jurisdiction of computer crimes. In their working report, the Commission expressed that

> 'If a hacking offence [was] created, what jurisdiction rules should govern its operation? Should a specific jurisdictional rule be created, or should the matter be left to the common law? Should courts [had] jurisdiction if either a person in England and Wales [obtained] unauthorised access to a computer abroad, or if a hacker abroad [obtained] unauthorised access to a computer in England and Wales?'[754]

As a response to these issues, the jurisdiction principle attached to cybercrime has an extra-territorial effect. Analysing section 4(1), 'even if no element of the offence occurred in that country and/or the defendant was not present in that country, so long as there is at least one "significant link" with the jurisdiction'.[755] By saying 'significant link', section 5 of the ECMA explains it as either the offender was in the 'home country' when he carried out any

---

[751] Section 4(1) of the Computer Misuse Act.

[752] Section 4(6) of the Computer Misuse Act.

[753] Section 5(1A) of the Computer Misuse Act.

[754] The Law Commission, *Computer Misuse working Paper No. 110*, [8.7(d)].

[755] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, pp. 408-409.

relevant act for conviction of the offence or any result (e.g. the unauthorised access or distribution of hacker tools) occurred in the 'home country'.[756]

5.4 The Scope of Cybercrime

The terms used ranged from 'computer crime'[757] to 'net-crime',[758] from 'hi-tech crime'[759] to 'cybercrime'.[760] The main distinguishing feature between these terms is their scopes, in other words, the kind of conducts that be regarded as cybercrime.

Nonetheless, all of these terms have flaws, according to the Law Commission. For instance, 'net-crime' is defined as 'criminal or otherwise malicious activity utilising or directed towards the internet and/or information technology applications';[761] it stretches the scope of the crime beyond desktop or laptop activities and encompasses all forms of networked devices.[762] However, this may lead to over incrimination by including all networked devices, such as Global Positioning System devices used in cars. The term 'hi-tech crime' is rejected because any technology, such as biotechnology, may also fall into its range. Regarding the term 'computer crime' now used in legal instruments, it is the most frequently used term, and is deemed to encompass a wide range of offences, such as virus dissemination, hacking and computer facilitated terrorist crimes.[763] However, there is neither an authoritative definition of 'computer crime' nor a widely accepted interpretation in practice. In this context, in order to define 'computer crime', some people attempt to define 'computer' first.

However, with respect to the issue 'what is computer', the situation is similar: there is no consensus on it. A comprehensive definition may lead to over-incrimination, yet a narrow definition may result in a situation that newly emerged acts relating to computers is not

---

[756] Section 5 of the Computer Misuse Act.

[757] Ian Walden, *Computer Crime and Digital Investigations*, Oxford: Oxford University Press, 2007.

[758] Sheridan Morris, 'The Future of Netcrime Now: Part 1-Threats and Challenges', Home Office Online Report 62/04.

[759] Paul Norman, 'Policing "Hi-tech" Crime within the Global Context: the Role of Transnational Policy Networks', in David Wall (ed.), *Crime and the Internet—Cybercrimes and Cyberfears*, London: Routledge, 2001, pp. 184-194.

[760] David Wall, 'The Internet as a Conduit for Criminals', in Pattavina April, *Information Technology and the Criminal Justice System*, California: Sage, 2005.

[761] Sheridan Morris, 'The Future of Netcrime Now: Part 1-Threats and Challenges', Home Office Online Report 62/04.

[762] *Ibid.*

[763] Paul Barton and Viv Nissanka, 'Comparative Computer Crime: Cyber-crime – Criminal Offences or Civil Wrong?' *Computer Law and Security Report*, vol. 19 5(2003): 401-405, p. 401.

covered, and thus cannot be punished. To keep a balance between over-incrimination and letting the actors escape punishment, some scholars and legislators suggested to leave it undefined but explicitly listed certain items not considered to be a computer,[764] as the US has done in its federal legislation.[765] For instance, in a working report, the Law Commission proposed that although 'a detailed, technical definition of a "computer" would be undesirable, a partial negative definition excluding certain items might be helpful'.[766]

At the same time, the Law Commission admitted that 'computer' was 'in general easy to recognise but very difficult to define'.[767] Thus, it also proposed another approach on this issue: to leave the term 'computer' undefined,[768] which is the current approach England takes. In the preparation stage of the ECMA 1990, the Law Commission expressed its hesitation of defining 'computer'. In its working paper the Law Commission admitted that 'it would be better not to attempt to define "computer" in any legislation that may be recommended',[769] because

> '… all the attempted definitions that we have seen are so complex, in an endeavour to be all-embracing, that they are likely to produce extensive argument, and thus confusion for magistrates, juries and judges…'[770]

Although leaving the 'computer' undefined, the term 'computer' could not be left open to the judges to decide; at least some guidance of interoperating 'computer' must be proposed. In this sense, the Law Commission recommended the adoption of the ordinary meaning of the term 'computer'.[771] If this recommendation were adopted, the ordinary meaning of computer would apply, and legislators would guide judges as to whether an item is a computer or not at

---

[764] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 53.

[765] The Law Commission, *Computer Misuse working Paper No. 110*, [6.23].

[766] *Ibid.*

[767] *Ibid.*

[768] For different opinions, see e.g. Tom Mulhall, 'Is the Threat of the High-Tech Computer Hacker an Exaggerated One, Or Was There Ever a Need for the Computer Misuse Act 1990?' *Computer Fraud and security*, 12(1996): 11-18, pp. 13-14. Tom Mulhall points out the strange that there is no definition of 'computer' in Act dealing with computer crime. He also argues in this article that there was no need to enact a special criminal regulation to deal with computer misuses, and the existing criminal Acts are 'more than capable' for crimes against or by computers.

[769] *Ibid*.

[770] The Law Commission, *Computer Misuse No. 186* (1989), [3.39].

[771] The Law Commission, *Computer Misuse working Paper No. 110*, [6.23].

the same time. Not surprisingly, broad applications can be made with such an approach, considering the wide discretion enjoyed by the judges.

The APIG is also a supporter of the current approach, i.e. leaving 'computer' untouched. When reviewing the Computer Misuse Act in 2004, the APIG received a number of proposals suggesting defining 'computer' in the Act. The APIG, like the Law Commission, rejected these suggestions by arguing that the absence of a definition had not led to more problems in practice and that judges did a good job in interpreting it.[772] In the end, the APIG recommended that there should be no change with respect to the approach towards defining 'computer'.[773]

In addition, the Home Office suggested of leaving the term 'computer' undefined because it found that there had not been any occasion where the courts failed to define the term 'computer'. It stated that

> 'We recommended that the Government resist calls for words such as "computer" to be defined on the face of the Computer Misuse Act and continue with the scheme whereby they [would] be understood by the courts to have the appropriate contemporary meaning.'[774]

Thus, the attempt of defanging 'computer crime' through defining 'computer' does not succeed, and both of these terms are left open to judges. At the same time, the Law Commission admitted that for cases that could 'only be committed with the aid of a computer' (i.e. the genuine computer crimes), they 'would then accurately be called a computer crime'.[775]

5.5 Summary

As the historical review and its current cybercrime legislation show, England chooses to introduce new provisions and Acts to tackle with those 'genuine cybercrime' and rely on its existing criminal provisions dealing with traditional crimes facilitated by computers. This

---

[772] 'APIG Computer Misuse report', Legal and Political News Affecting ISPs and Internet Users Public Affairs', 30 June 2004, available at https://publicaffairs.linx.net/news/?p=110. Last visited March 2015.

[773] The Law Commission, *Computer Misuse working Paper No. 110*, [6.23].

[774] 'Revision of the Computer Misuse Act-Report of an Inquiry by the All Party Internet Group', June 2004, [15]

[775] The Law Commission, *Computer Misuse working Paper No. 110*, [1.6].

approach, as suggested by its Law Commission, is called the 'half-way' approach, meaning that 'rejecting the creation of wholly new offences, except where these are absolutely necessary, but being prepared to contemplate the widening of existing general offences (by, for example, the amendment of definitions or conditions) in order to make these existing offences more appropriate for incidents of computer misuses'.[776] Although recommended by the Law Commission, one of the issues regarding this approach is that the traditional provisions were certainly not drafted with the potential functions in mind, since most of the provisions were enacted before the appearance of computers and computer networks. Applying them in the new era challenges many criminal principles such as that only tangible things can be stolen or damaged, and only human beings can be deceived. Still, England sticks to this halfway approach in the last three decades.

The England Computer Misuse Act introduces the new offences that cannot be covered through stretching traditional criminal laws, and the Act has been amended in 2006 and 2015 respectively, in order to meet new requirements presented by the development of information technology.

In this process, case law and judges in England did not play as prominent a role as in other fields of laws. As the front line of the judicial proceedings, English judges are expected to take the initiative to make new laws against cyber wrongdoings, since they do not have the opportunity of leaving the disputes in trials to the legislators. However, facts show this expectation's inadequacy. As mentioned, the traditional provisions were drafted before the birth of the computer, and even the ECMA has always fallen behind the changes of computer crimes. In this regard, the interpretations made by the judges are for most of the time 'far from far-reaching'.[777] As Lord Reid expressed in the case *Myers v. DPP*,

> '[if] we are to give a wide interpretation to our judicial functions, questions of policy cannot be wholly excluded, and it seems to me to be against public policy to produce uncertainty. The only satisfactory solution is by legislation following on a wide survey of the whole field…'[778]

[776] The Law Commission, *Computer Misuse working Paper No. 110*, [4.5].

[777] Colin Tapper, 'Judicial Attitudes, Aptitudes and Abilities in the Field of High Technology', *Monash University Law Review*, vol. 15 3(1989): 219-228, p. 220-223.

[778] *Myers v. Director of Public Prosecutions*, [1965] A.C. 1001, 1022.

What's more, considering the absence of the definition on 'cybercrime' and 'computer', the situation judges are facing is even more challenging. Thus, judges prefer to wait for the legislative guidance as regards to the new forms of cybercrime, rather than to stretch the laws without in-depth research.

Generally speaking, the legislative approach taken by England is relatively conservative. Several facts reflect this attitude, including the reliance on traditional criminal laws, the only two Amendments it enacted to the ECMA and one of which primarily raises the punishment attached, and the enforcement powers granted to judicial organs.[779]

Concerning this conservative attitude, the effectiveness of the ECMA remains the central position of relevant discussions. Some scholars once suggested that a criminal act as such is not necessary; traditional criminal laws are sufficient.[780] Some, on the contrary, express their concern that the resources and technical expertise enjoyed by law enforcement agencies are too limited, and this situation may ultimately lead to a failure when combating computer crimes.[781] Some scholars further recommend an alternative mechanism that can more appropriately regulate this problem,[782] and political intervention may eventually be proven more effective than the judgement of legal professionals.[783]

In sum, although there have been criticisms and disagreements, the half-way approach has proved its value both in theory and practice, as shown by the division of data and computer, and the division of computer as the target and computer as the tool. In the beginning, the ECMA protected data; after noticing the function of computer also became one of the targets, the ECMA takes computer as a subject as well. Accordingly, sections 1 and 2 protect data, and thus mere hacking is criminalised under the ECMA. Section 3 protects the function of

---

[779] Home Office, *Cyber Crime Strategy cm 7842*, UK: The Stationery Office Limited, 2010, [37].

[780] See e.g. Tom Mulhall, 'Is the Threat of the High-Tech Computer Hacker an Exaggerated One, Or Was There Ever a Need for the Computer Misuse Act 1990?' *Computer Fraud and security*, 12(1996): 11-18. The author suggests in this article that a large quantity of computer frauds is an exception, and hackings are to a large extent exaggerated.

[781] See e.g. Kit Burden and Creole Palmer, 'Internet Crime: Cyber Crime – A New Breed of Criminal?' *Computer Law and Security Report*, vol. 19 3(2003): 222-227. The authors compare this situation as 'the Dutch boy with his finger in the dyke', and express that law enforcement agencies cannot combat computer crimes with such limited resources and technical expertise.

[782] See Stefan Fafinski, 'Computer misuse: The implications of the Police and Justice Act 2006', *Journal of Criminal Law*, 1(2008): 53-66.

[783] See Yaman Akdeniz, Nick Taylor and Clive Walker, 'Regulation of Investigatory Powers Act 2000 (1): BigBrother.gov.uk: State Surveillance in the Age of Information and Rights', *Criminal Law Review*, 2(2001): 73-90.

computer, and thus DoS attack is criminalised even under a few occasions no access is conducted. In a rapidly developed field, a systematic approach like this can guide judges applying relevant criminal laws consistently.

Chapter 6 The Cybercrime Legislation in Singapore

6.1 Introduction

This Chapter intends to discuss the Singapore legislation on cybercrime and unveil the approach it takes against cyber wrongdoings. The Singapore legislation on cybercrime contains one specific Act and four Amendments. Having considered that it was inappropriate to use the Singapore Penal Code (hereafter the Singapore PC) to deal with computer misuse,[784] Singapore promulgated the (Singapore) Computer Misuse Act in 1993 (hereafter the SCMA 1993), and introduced a new category of crime - computer crime. Later, as being criticised as lack of clarity and 'seemingly open disregard' of individual rights,[785] Singapore enacted four Amendments, in 1996, 1998, 2003 and 2013 respectively.

To explore the trends of the Singapore legislation on cybercrime, 6.2 starts with a historical review of the Singapore Computer Misuse Act. 6.3 analyses the current legislation concerning computer crime both substantively and procedurally (regulations with respect to jurisdiction). In 6.4, the scope of cybercrime in Singapore, together with a special issue - the enforcement power granted to officials, are discussed. In the end, 6.4 summarises the characteristics and the legislative approach of the Singapore cybercrime legislation.

6.2 Historical Review of the Cybercrime Legislation in Singapore

As mentioned, the first piece criminalising cyber wrongdoings in Singapore is the SCMA 1993. Soon after, due to the rapid development of information technology, Singapore found the SCMA 1993 inapplicable either for lack of substantial provisions or lack of enforcement measures. Therefore, Amendments to the SCMA are enacted in 1996, 1998, 2003 and 2013 respectively. Since there was limited discussion on cybercrime before the promulgation of the SCMA 1993, the history of the SCMA can be divided into two periods: (1) from 1993 to 1996, applying the first computer specific legislation, and (2) after 1996, expansions and amendments.

---

[784] See *Parliamentary Debates, Singapore Official Reports*, 28 May 1993, cols. 300 – 301.

[785] See Indira Mahalingam and Katherine S. Williams, 'A Step Too Far in Controlling Computers? The Singapore Computer Misuse (Amendment) Act 1998', *International Journal of Law and Information Technology*, vol. 8 1(2000): 48-64, pp. 48-49.

6.2.1 From 1993 to 1996: the first computer specific legislation

The SCMA 1993 is the first legislation criminalising computer misuses in Singapore, incorporating those offences 'which [are] unique to computer technology'.[786] It was passed 'to make provision for securing computer material against unauthorised access or modification and for matters related thereto'.[787] The SCMA 1993 contained three parts: part I Preliminary, part II Offences, and part III Miscellaneous and General.

As the first step, part I defined and explained some key terms used in the SCMA 1993, especially those technical ones such as 'computer', 'data', and 'electronic device'. Taking the Computer Misuse Act of England as its legislative source key,[788] the SCMA 1993 borrowed the definitions and explanations directly from its English counterpart only with one exception 'computer',[789] since England left this term undefined in its Computer Misuse Act.

Part II, sections 3 to 7, was the core of the SCMA 1993. It is interesting to point out that sections 3, 4 and 5 were borrowed from sections 1, 2 and 3 of the England Computer Misuse Act 1990,[790] and section 6 resembled section 301.2 of Canada Criminal Code – unauthorised use of a computer.[791]

Among these four provisions, section 3 criminalised knowingly using a computer to secure access to program or data without authorisation. Offences under section 4 were in principle the same conduct as that under section 3, yet carrying a heavier punishment for the intent to commit or facilitate the commission of other offences. To be specific, section 4 criminalised

---

[786] *Parliamentary Debates*, Singapore Official Report, col. 301.

[787] Long Title of the Singapore Computer Misuse Act, 1993.

[788] Legislative Source Kay of Computer Misuse Act (Chapter 50A).

Unless otherwise stated, the abbreviations used in the references to other Acts and statutory provisions are references to the following Acts and statutory provisions. The references are provided for convenience of users and are not part of the Act:

UK CMA 1990	:	United Kingdom, Computer Misuse Act 1990 (c. 18)
Canada CLAA 1985	:	Canada, Criminal Law Amendment Act 1985 (c. 19)
S Aust. EA 1929	:	South Australia, Evidence Act 1929

[789] See Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, p. 265. For information on the phenomenon that England refused to set out a definition for *computer*, see Chapter 5 Cybercrime Legislation in England.

[790] See e.g. Katherine S. Williams and Indira Mahalingam Carr, 'The Singapore Computer Misuse Act – Better Protection for the Victims?' *Journal of Law and Information Science*, vol. 5 2(1994): 210-226.

[791] Section 6 of the SCMA 2013; *cf* section 301.2 of Canada Criminal Code 1989.

unauthorised access with the purpose of committing or facilitating further crimes 'involving property, fraud, dishonesty or which caused bodily harm'.[792] Section 5 criminalised behaviours that modify the contents of computers without authority. Section 6 criminalised unauthorised use or interception of computer services. However, section 6 was arguably overlapped with sections 3 and 4. It was argued that no interception or use stated in section 6 could be conducted without securing access to a computer system or modifying data stored on it, i.e. the acts proscribed by sections 3, 4 and 5.[793] This issue will be clarified in 6.3 Current Cybercrime Legislation in Singapore. Section 7 penalised abetting and attempting to commit the offences under the SCMA 1993, performing as a measure to strengthen the impact of the SCMA 1993.

Part III of the SCMA 1993 incorporated procedural matters, including setting up the extra-territorial application scope of the SCMA,[794] and empowering the police to have access to or inspect the operation of any computer that they had reasonable cause to suspect it had been involved in offences under the SCMA.[795]

Generally speaking, the SCMA establishes the framework of cybercrime legislation in Singapore. However, it was criticised for its lack of clarity of definitions and provisions, the consequent vague application scope, and the overlaps among sections.[796] In this context, a proposal for amending the SCMA 1993 was raised and adopted shortly after.

6.2.2 After 1993: expansions and amendments

6.2.2.1 The Evidence (Amendment) Act 1996: an effort to enhance administrative powers

As a response to the criticism that the definition of 'computer' was lacking clarity, the Evidence (Amendment) Act 1996 (hereafter the SEAA 1996) substituted one paragraph under

---

[792] Section 4(2) of the Singapore Computer Misuse Act 1993. This section was widely criticised for its lack of clarity. See e.g. Katherine S. Williams and Indira Mahalingam Carr, 'The Singapore Computer Misuse Act – Better Protection for the Victims?' *Journal of Law and Information Science*, vol. 5 2(1994): 210-226.

[793] See e.g. Assada Endeshaw, 'Computer Misuse Law in Singapore', *Information and Communication Technology*, vol. 8 1(1999): 5-33, p. 14. In this article the author argues that section 6 introduced a novel concept of using or intercepting a computer service without authority, and such an act was as the same as theft of computer service or time. He also emphasised that section 6 should be merged into section 3 and 4 because every authorised access to a computer or data held on them was likely to result in theft of service or time of the computer.

[794] Section 8 of the SCMA 1993.

[795] Section 14 of the SCMA 1993.

[796] Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331.

the definition of 'computer' - 'such other device as the Minister may by notification prescribe'.[797] From this substitution one can notice that the SEAA 1996 does not reply directly to the criticism on the clarity, neither did it explain the 'computer' in further detail. Rather, it enhanced the flexibility of the term by granting the Minister the right to extend the list by official notification. This amendment was commented as mainly to strengthen administrative powers in the field of criminalising cyber wrongdoings.[798]

6.2.2.2 The Computer Misuse (Amendment) Act 1998: introductions of new offences and increases of penalties

Since the Evidence (Amendment) Act 1996 did not clarify the definitions and provisions, as well as to respond to the inability of the SCMA to regulate newly emerged computer misuses such as DoS attacks and trafficking access code, the Singapore Computer Misuse (Amendment) Act 1998 (hereafter the SCMAA 1998) was enacted. For the first, the SCMAA 1998 intended to further strengthen 'the level and nature of the protection of computer systems' that had already been emphasised under the Evidence (Amendment) Act 1996. For the second, it also intended to enhance the protection for 'protected computer'.[799] Therefore, the SCMAA 1998 enacted a new version of section 4, introduced two new offences with regard to unauthorised obstruction of the use of a computer and disclosure of access code, and increased the punishment on unauthorised access to the 'protected computers'.

Firstly, the SCMAA 1998 affirmed the change in the definition of 'computer' made by the Evidence Act 1996. It then introduced a definition of 'damage to a computer or the integrity or availability of data, a program or system, or information', including 'material loss, modification or impairment on medical records, physical injury or death of people, and public health or public safety'.[800]

Secondly, the SCMAA 1998 enacted a new section 4, in which exceeding their authority to commit further crimes were outlawed. Before the SCMAA 1998, the issue that whether

[797] Section 3 of the SCMA 1996.

[798] Indira Mahalingam and Katherine S. Williams, 'A Step Too Far in Controlling Computers? The Singapore Computer Misuse (Amendment) Act 1998', *International Journal of Law and Information Technology*, vol. 8 1(2000): 48-64, p. 50.

[799] Assada Endeshaw, 'Computer Misuse Law in Singapore', *Information and Communication Technology*, vol. 8 1(1999): 5-33, p. 16.

[800] Section 2(1) of the SCMA 1998.

section 4 applies to accesses 'exceeding authority' was uncertain.[801] For instance, one staff of a cinema used his authority to access the cinema cash card computer system and made some gains by altering computer records. Although reported as computer misuse, this actor was prosecuted under the Singapore Penal Code for criminal breach of trust because of the unclear coverage of section 4. In the Parliamentary debate, this issue was heatedly discussed and addressed. One of the speakers supported the original section 4 by suggesting that the original intent of the SCMA was to punish unauthorised access. If 'exceeding authority' was to be criminalised as a separate offence, the original intent was subsequently amended which seemed unnecessary and unfavourable.[802] To further illustrate that it was not necessary to charge the offenders for a computer misuse apart from the offence it intended to commit or facilitate, Mr Chin Tet Yung, another supporter of the original section 4, suggested that the offenders could be charged with the offences that their access was intended to facilitate.[803] In addition, Mr Chin Tet Yung further pointed out that when the authorised offender obtained access to do an unauthorised act, he was already using a computer in an unauthorised way and therefore misused that computer.[804] In responding to this opinion, the then Minister Mr. Wong Kan Seng emphasised that the idea of the new section 4 was not to prosecute the use of a computer for a proper and lawful purpose, but to remove the uncertainty that a person who had authority to access a computer might find himself guilty of an offence if he were to use the computer to commit a further crime.[805] Besides, he pointed out that prosecuting the offenders under other laws because of the intended crime such as theft and extortion was admittedly practical, but it was more appropriate to update the law and prosecute them under the SCMA if they actually abused their authority in using the computer.[806] This statement also indicates that Singapore would like to use the SCMA to deal with those misuses committed through using computer rather than replying on traditional criminal provisions, to emphasise the illegal nature of unauthorised usage of the computer.

---

[801] *Parliamentary Debate, Singapore Official Report,* 30 July 1998, cols. 398.

[802] *Ibid*, cols. 401.

[803] *Ibid*, cols. 401-402.

[804] *Ibid*, cols. 408-409.

[805] *Ibid*, cols. 412-413.

[806] *Ibid.* The then Minister also assured that such act would not be charged twice for the same offences based on the same facts. Like the example of extortion, the offender would only be charged once, and under the SCMA if this change were passed. Judgements on later cases show that the offender faced at least two charges, one under section 4, and the other one under provisions regarding the crimes they intended to commit. See e.g. *Public Prosecutor v. Law Aik Meng* [2007] 2 SLR 814; [2007] SGHC 33, and *Navaseelan Balasingam v. Public Prosecutor* [2007] 1 SLR 767; [2006] SGHC 228.

Thirdly, two new offences created by the SCMAA 1998 were unauthorised obstruction of the use of computer (new section 6A) and unauthorised disclosure of access code (new section 6B).[807] Section 6A was to penalise the so-called E-mail bombing, and section 6B was to criminalise unauthorised disclosure of passwords or access codes.[808]

The fourth change was the increased penalties imposed on cyber offences, especially on the offences committed on a 'protected computer'. Acting as a limitation to the enhanced penalties, the threshold of offences under relevant sections had been raised correspondingly.[809] The term 'protected computer' introduced by section 6C referred to the computers or programs or data that are 'used directly in connection with or necessary for

> '(*a*) the security, defence or international relations of Singapore;
>
> (*b*) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;
>
> (*c*) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or
>
> (*d*) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services'.[810]

It is noteworthy that the requisite knowledge from (a) and (d) was presumed, meaning that the offender was presumed to know the device he accessed was for national security or other functions listed, unless the contrary was proved.[811] The enhanced penalty for protected computers, together with the presumption of requisite knowledge, argued by Endeshaw, jointly indicated 'a determination by the government to stamp out any attempts at intrusion into sites considered vital to the economic and national security of Singapore'.[812]

---

[807] After the 2007 Revised Edition of the SCMA, sections 6A, 6B and 6C are renumbered as sections 7, 8 and 9. The original section 7 on abets and attempts are renumbered as section 10.

[808] *Parliamentary Debate, Singapore Official Report,* 30 July 1998, cols. 398-399.

[809] Assada Endeshaw, 'Computer Misuse Law in Singapore', *Information and Communication Technology*, vol. 8 1(1999): 5-33, p. 17.

[810] Section7 of the SCMA 1998.

[811] *Ibid*.

[812] Assada Endeshaw, 'Computer Misuse Law in Singapore', *Information and Communication Technology*, vol. 8 1(1999): 5-33, p. 18.

6.2.2.3 The Computer Misuse (Amendment) Act 2003: an expansion of enforcement powers

Considering the enforcement measures listed in the SCMA were not enough to prevent threats to computers, in 2003 the legislature again enacted the Singapore Computer Misuse (Amendment) Act 2003 (hereafter the SCMAA 2003). It inserts a new provision under section 12 as 12A, stating that an authorised police officer had the power to impose an on-the-spot fine of up to $3000 on a person reasonably suspected of having committed an offence of this category. It inserts a new provision as 15A under section 15, aiming at preventing threats to national security and essential services,[813] and others. Section 15A is intended to authorise the Minister to take measures to prevent a threat to a computer for the purpose of national security. If necessary, the Minister can also authorise any person or organisation to take such a measure.[814] This effort, as suggested by some, reflected the same purpose as legislative changes in many Western countries - against terrorism.[815]

6.2.2.4 The Computer Misuse (Amendment) Act 2013: further expansions of enforcement powers

The Computer Misuse (Amendment) Act 2013 was enacted to entitle the government to take measures to prevent, detect and counter attacks on critical information infrastructure (hereafter the CII)[816] to ensure Singapore's cyber security, national security, essential services, defence or foreign relations. Amendments made by the SCMAA 2013 are mainly regarding enforcement powers for the purpose of strengthening national interests.

Firstly, the SCMA was renamed as Computer Misuse and Cybersecurity Act[817], and its long title was changed to reflect the attention paid to national interests. As suggested by the second Minister of Home Affairs, this Amendment '[would] accurately reflect the scope of the Act,

[813] 'Essential service' under section 15A was referred to as '(a) services directly related to communications infrastructure, banking and finance, public utilities, public transportation or public key infrastructure; and (b) emergency services such as police, civil defence or medical services'. Section 3 of SCMA 2003.

[814] Section 15A of the SCMA 2003.

[815] See e.g. Christine Doran, 'Politics, the Net, and Gender in Singapore', *Review of History and Political Science*, vol. 2 6(2014): 1-16.

[816] 'Critical information infrastructure' refers to 'systems which are necessary for the delivery of essential services to the public in various key sectors'. See *Parliamentary Debate, Singapore Official Report*, 14 January 2013, 3. 03 pm.

[817] Considering that most of the materials on cybercrime legislation in Singapore adopt the term 'Computer Misuse Act', this thesis sticks to it, rather than the new name, in order to avoid misunderstanding.

including its objective of securing Singapore against cyber threats that may endanger our national interests'.[818]

Secondly, this Amendment replaced 15A with a new version – the one delegating more powers to government officers and even to individual persons.[819] As commentated by the members of the Second Reading[820] of the Computer Misuse (Amendment) Bill 2013, the new 15A would 'empower and allow the Minister to order a person or organisation to act against any cyber-attack even before it has begun',[821] and the immunity under section 15A (6) would 'confer criminal and civil immunity on anyone who in good faith implements any measure or acts according to directions he receives under the Act'.[822] Additionally, a new offence is created by this Amendment under 15A(4), to achieve the aims set out in its long title, especially to prevent crimes potentially violating national security.[823]

To sum up, Singapore started to arm both its courts and law enforcement agencies, and even relevant organisations from the early 1990s to fight against computer crime, following England and some other jurisdictions. Nonetheless, whereas England reacted actively in establishing legislation on cybercrime, it remained relatively passive in amending its Act and granting law enforcement agencies powers. Compared with England, Singapore seems more aggressive. This observation can be manifested by the four Amendments to the SCMA and the powers allocated to government officers. More importantly, as shown in both the

---

[818] *Parliamentary Debates, Singapore Official Reports*, 14 January 2013, 3.03 pm. The Long title was amended from 'An Act to make provision for securing computer material against unauthorised access or modification and for matters related thereto' to 'An Act to make provision for securing computer material against unauthorised access or modification, *to require or authorise the taking of measures to ensure cybersecurity,* and for matters related thereto'.

[819] See e.g. *Parliamentary Debates, Singapore Official Reports*, 14 January 2013, 3.17 pm-3.22 pm the speeches given by Mr Hri Kumar Nair and Mr Christopher de Souza.

[820] With respect to the law-making process in Singapore, a bill is introduced to the Parliament without debate, as the First Reading. After this introduction, the bill will be read by the Members of Parliament (hereafter the MPs) in charge for a second time (not the Second Reading). During this stage the MPs in charge have an opportunity to debate on the general principles of the bill. To be specific, the bill has been read twice before it goes to the Second Reading. Then, if the MPs in charge think the bill is beneficial to Singapore, they will vote for it and the bill will get an opportunity for the Second Reading. In the Second Reading, the bill progresses to the Committee of the Whole Parliament or to a Select Committee comprising several MPs to examine it section by section. MPs who support the bill in principle but do not agree with certain clauses can propose amendments to those clauses at this stage. Following its report back to the House, the bill will go through the Third Reading where only minor amendments will be allowed before it is passed. For more details see 'What We Do', available at https://www.parliament.gov.sg/what-we-do. Last visited April 2016.

[821] *Parliamentary Debates, Singapore Official Reports*, 14 January 2013, 3.22 pm.

[822] *Ibid*, 3.17 pm.

[823] See e.g. *ibid.*

Parliamentary debate and scholars' analysis, to protect the national interest serves as the main reason for this aggressive approach.

6.3 Current Legislation on Cybercrime

Singapore has a number of legal statutes that apply to computer misuse and computer related misuses, including the Singapore Computer Misuse Act, the Singapore Penal Code, the Singapore Undesirable Publications Act, and others. Among these statutes, the SCMA, as introduced above, is the primary legal instrument against cybercrime, including the crimes targeting computer, and the traditional crimes facilitated by computers.

6.3.1 Offences against the security of computer

Learning from England and Canada, the SCMA contains 6 sections criminalising acts that threatening the security of data and computer, including acts that unauthorised access to computer materials (section 3), access with intent to commit or facilitate commission of offence (section 4), unauthorised modification of computer material (section 5), unauthorised use or interception of computer service (section 6), unauthorised obstruction of use of computer (section 7), and unauthorised disclosure of access code (section 8).

6.3.1.1 Access offence

Sections 3 and 4 of the SCMA criminalise access offences. Specifically, section 3 criminalises 'mere hacking'. That is, knowingly causing a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer.[824] Section 4 criminalises access with an intention to commit or facilitate the commission of a criminal offence involving property, fraud, dishonesty or which causes bodily harm.[825] To understand these two provisions, four key elements are analysed, including 'computer', 'access', 'authorisation', and 'fault element'.

(1) Computer

Computer is defined as

> 'an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or

[824] Section 3(1) of the SCMA 2013.

[825] Sections 4(1) and (2) of the SCMA 2013.

> storage functions or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include —
>
> (*a*) an automated typewriter or typesetter;
>
> (*b*) a portable hand held calculator;
>
> (*c*) a device similar to those referred to in paragraphs (*a*) and (*b*) which is non-programmable or which does contain any data storage facility;
>
> (*d*) such other device as the Minister may by notification prescribe'.[826]

This definition shares a great similarity with the US definition.[827] In fact, it follows the approach the US takes when defining 'computer' to tackle with future changes. Namely, it contains two parts. The first part characterises what devices can be deemed as a computer, and the second part excludes certain devices that are not a computer for its purpose.[828]

The American scholars maintain that this exclusive definition is certain and clear, and the clarity of the status of certain devices can to a large extent avoid ambiguity.[829] However, considering potential future advances in this field, this definition needs to be precise and is at the same time broad and technologically neutral. Therefore, it is criticised by Singaporean scholars as casting a net too wide, and fails to exclude some now trivial devices such as digital cameras because they may play a role significant enough to harm the society in the future.[830] Taking this criticism into consideration, some scholars suggest learning from England, as it does in its domestic law, to leave the court to develop criteria when deciding what types of devices could be regarded as a computer under this definition.[831]

---

[826] Section 2(1) of the SCMA 1996.

[827] See e.g. Indira Mahalingam and Katherine S. Williams, 'A Step Too Far in Controlling Computers? The Singapore Computer Misuse (Amendment) Act 1998', *International Journal of Law and Information Technology*, vol. 8 1(2000): 48-64, p. 49. For discussions and research on the American definition of *computer*, see Chapter 4 Cybercrime Legislation in the US.

[828] Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, pp. 267-268.

[829] Joseph M. Olivenbaum, '<Ctrl> <Alt> <Del>: Rethinking Federal Computer Crime Legislation', *Seton Hall Law Review*, 27(1997): 574-641, pp. 619-621.

[830] Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, p. 268.

[831] *Ibid*, p. 269.

(2) Access

In section 2(2) of the SCMA, *securing access by causing a computer to perform any function* is defined as

> '(*a*) alters or erases the program or data;
>
> (*b*) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
>
> (*c*) uses it; or
>
> (*d*) causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner), and references to access to a program or data (and to an intent to secure such access) shall be read accordingly'.

In addition, 'function' is defined in section 2(1) to include 'logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer'.

These two definitions are defined in a way that practically any act of operating a computer would fall within its regime, no matter whether physically or through using another computer.[832] For instance, a simple act of switching on the computer would cause that computer to function and therefore satisfy the element of 'securing access by causing a computer to perform any function'.[833]

Moreover, as rightly pointed out by Lee Gen-Min, if read these two definitions together with the broad term 'computer', 'the physical act element of this offence can be easily satisfied by conduct which would not ordinarily be considered to be 'use' or 'operation' of a 'computer'.[834] For instance, turning on an iPad without authority would satisfy the physical element of this provision simply because it will cause the iPad – a computer - to respond and compute logically. What makes the broad definition of 'access' even worse is the fact that

[832] Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, p. 274.

[833] See e.g. Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 68.

[834] Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, p. 274.

since this physical element is defined by reference to the wrongdoer's conduct rather than consequences, such an offence is finished at the very point that the iPad starts to compute.[835]

(3) Authorisation

Copied directly from the wording in England Computer and Misuse Act, section 2(5) of the SCMA explains the concept of 'access of any kind by any person to any program or data in a computer unauthorised or done without authority' by providing scenarios that:[836]

> '(*a*) he is not himself entitled to control access of the kind in question to the program or data; and
>
> (*b*) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled'.[837]

To put the explanation in a simpler way, in situations where the access is conducted by the Entitled Person or by a person to whom the Entitled Person has given consent, this access is authorised; otherwise it is not.

As rightly pointed out, this explanation is established on the identification of a person 'entitled to control across of the kind in question' (hereafter the Entitled Person). One issue thus emerges that in a situation where there is no Entitled Person or there is more than one Entitled Person, no one can give consent, or it is uncertain that who has the right to give consent. In cases where there is no Entitled Person to a particular computer or program or data, are all accesses unauthorised? In the scenarios that one person owns a computer, while another person enjoys the right to use a program in that computer, should the Entitled Person be both of them, or any of them? In other words, must an actor obtain consent from both of them or any of them?[838] To address these questions and to decide who the Entitled Person is

---

[835] *Ibid*, pp. 274-276.

[836] Such explanations are criticised by some scholars because they leave no space to case law, which leads to ineffectiveness of the statutes. See e.g. Terry Johal, 'Controlling the Internet: The Use of Legislation and Its Effectiveness in Singapore', in *15th Biennial Conference of the Asian Studies Association of Australia, Canberra, 2004.*

[837] Section 2(5) of the Singapore Computer Misuse Act 2013; *cf.* section 17(5) of the England Computer Misuse Act 2006.

[838] Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, pp. 276-282. In this article the author uses an example of network provider and the owner of a network server to illustrate the issue in question. To be specific, in cases where the network provider uses a third party's network server to run a website, is it the network provider or the owner of the network server who is entitled to control access to the server?

with respect to a certain computer, program or data, a look at what is meant to be 'entitled' is necessary. However, the SCMA 2013 is silent on this issue and barely provides any assistance. Consequently, the concept of 'entitled' may be flexible and depend on circumstances of the case under consideration.[839]

(4) Fault element

The fault element of section 3 is 'knowingly'. Specifically, it contains three parts: (1) the offender's act will cause a computer to perform any function, (2) such an act is without right, and (3) such an act is done for the purpose of securing access to any program or data held in a certain computer.[840] The offender does not need to target a certain device or a certain kind of device, and the targeted programs, systems or data neither needs to be stored permanently or merely temporarily.[841]

This element can be interpreted quite broadly. For instance, with this fault element, some scholars have argued that whenever there was a computer being caused to perform any function, it would be considered as a crime with such a fault element of section 3, unless the act was conducted recklessly or somehow inadvertently.[842]

Regarding the knowledge of 'computer', one situation may happen that an actor secures access to a device that ordinary people would not regard as computer (such as iPad), (1) he knows his act will cause the iPad to function, (2) he knows his act is without right, and (3) his act is done for the purpose of securing access to the iPad. In this scenario, since the actor does not know iPad belongs to computer, it is unclear that whether the fault element is satisfied.

Before resolving it in the cyber context, the issue of mistaken beliefs of fact in ordinary cases shall be explored first. Section 79 of the Singapore Penal Code sets out a defence stating that

---

[839] Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, pp. 276-282.

[840] Section 3 of the SCMA 2013. For the element of (3), some would argue that it is not clear if the word 'knowingly' as used in section 3 is intended to qualify the phrase (3), and it is not clear in the use of the word 'purpose' that a potential offender must know the probable result of his acts is obtaining access. See Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331.

[841] Section 3(3) of the SCMA 2013.

[842] Assada Endeshaw, 'Computer Misuse Law in Singapore', *Information and Communication Technology*, vol. 8 1(1999): 5-33, p. 13.

> 'nothing is an offence which is done by any person who is justified by law, or who by reason of a mistake of fact and not by reason of a mistake of law in good faith believes himself to be justified by law, in doing it'.[843]

Under this defence, an actor who behaves under a mistaken belief of fact would avoid an offence provided it was done in good faith. Operating as a defence to criminal liability, section 79 of the Singapore Penal Code assigns the burden of proving this defence to the defendant.[844] As a general defence ruled in the Penal Cose, these rules apply to computer misuse as well, meaning that if the defendant of computer misuse raises a defence that he mistakenly believes the device he operated is not a computer, his conduct would be excused if he can prove this claim.

Regarding the knowledge of 'access', the abovementioned defence also applies. That means it is not necessary to draw a clear line between knowingly or not: if such a defence is raised, the defendant must prove it.[845] For instance, an ordinary person may know that his act would lead to some use of computer, while he does not know this operation falls within the regime of the technical definition of 'access'. If he can prove his mistakes, he shall get no criminal punishment.

Regarding the knowledge of 'authorisation', when it comes to a situation where the actor secures access to a computer and mistakenly thinks he has the right or consent from the Entitled Person, it is also valid that if the defendant can prove his act was under a mistaken belief and in good faith, he would be excused from criminal liability.[846]

Section 4 of the SCMA 2013 differs from section 3 mainly on two elements: 'authorisation' and 'fault element'.

(1) Authorisation

Prior to the SCMAA 1998, the offence under section 4 could only be committed when the access was unauthorised. After 1998, section 4 became 'a broadly applicable preparatory style

---

[843] Section 79 of the Singapore Penal Code 2014.

[844] Regarding the burden of proof in Singapore, see Michael Hor, 'The Burden of Proof in Criminal Justice', *Singapore Academic Law Journal*, 4(1992): 267-309.

[845] Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, pp. 286-287.

[846] *Ibid.*

of offence' which can be used wherever a computer is involved with the intention to commit further crimes.[847] For instance, in the case *Public Prosecutor v. S Kalai Magal Naidu,*[848] the defendant caused the computer server of the Malaysian Banking Berhad (hereafter the Maybank) to perform a function to secure access to the program held in this computer server and inputted a debit of $8000.00 from Maybank account belonging to someone else, with the intent to commit an offence of criminal breach of trust as a servant. In cases as such, whereas the offender attempted to obtain access for funds he may face a charge under section 4. Besides, if he succeeded in obtaining funds, he may also face charges under the SPC for theft or other offences.[849]

(2) Fault element

It is stated in section 4(2) that an offence under section 4 must be committed to commit or facilitate offences involving 'property, fraud, dishonesty or which causes bodily harm punishable on conviction with imprisonment for a term of 2 years or more'.[850]

It was argued that the purposes listed under section 4(2) are not sufficiently clear. This argument is untrue. Given that section 4 of the SCMA corresponds to section 2 of the England Computer Misuse Act, its interpretation of this element in England shall be explored first. The English Law Commission Report, as shown in the Chapter on England, set out several sample offences to which this provision applies, including theft by hacking into a bank's computer system to remove or transfer funds, hacking to obtain confidential and personal information for blackmail, and hacking to cause physical injury to persons.[851] In Singapore, most of these situations can be dealt with by section 4, with exceptions such as cheating and the basic offence of causing hurt.[852] This is because these two carry a punishment of less than two year's imprisonment, yet the intended offence must carry a minimum two years' imprisonment.

---

[847] Gregor Urbas, 'An Overview of Cybercrime Legislation and Cases in Singapore', *Asian Law Institute Working Paper Series No. 001*, December 2008.

[848] *Public Prosecutor v. S Kalai Magal Naidu,* [2006] SGDC 226.

[849] Gregor Urbas, 'An Overview of Cybercrime Legislation and Cases in Singapore', *Asian Law Institute Working Paper Series No. 001*, December 2008, p. 15.

[850] Although section 4 was replaced in 1998, section 4(2) remains the same.

[851] The Law Commission, *Computer Misuse No. 186* (1989), [3.4]-[3.7].

[852] Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, pp. 291-292.

6.3.1.2 Data interference and system interference

Aiming at protecting the security of the computer and data, the SCMA provides two provisions on convicting misuses damaging it. Namely, section 5 criminalises unauthorised modifications of computer material, i.e. data interference, and section 7 criminalises unauthorised obstruction of the use of a computer, i.e. system interference.

Specifically, section 5 deals with unauthorised modification of the contents of a computer by technological means, such as deleting data stored on computers. Such conduct was a copy of mischief defined in section 425 of the Penal Code in cyber context,[853] except that the target of crimes under section 5 was not corporeal property, but information/data stored on the computer.

However, section 5 is overlapped to some extent with section 3, especially in a scenario where the offender hacked into a computer to modify data stored on it: hacking violates section 3 and modification violates section 5. The definition of 'modification' under subsection 2(7)(a) makes this situation even worse. 'Modification' includes 'any program or data held in the computer concerned is altered or erased',[854] yet alteration or erasure to programs or data also constitute 'secure access to a computer to perform any function' – the *actus reas* under section 3.[855] It is exactly the same act (alteration and erasure) that violates both sections 3 and 5.

Scholars hold different opinions towards this phenomenon. Endeshaw believes that it is 'clearly not an indication of bad draftsmanship, but of an inability to segment the offences and peg them to the level of gravity of wrong done or attempted'.[856] Nonetheless, his argument is immediately weakened by the fact that the penalties for these two provisions are the same where the offender causes serious damage.[857] On the contrary, Lee Gen-Min maintains that section 5 specifically targets misuses where a modification of data was committed without hacking into the computer it is stored on. For instance, a person uploads a

[853] *Ibid*, p. 266.

[854] Section 2(7) of the SCMA 2013.

[855] Section 2(2) of the SCMA 2013. It should be noted that although Singapore borrowed this provision from England, it differs with respect to the relation between basic hacking provision and modification provision. In England, modification to system or data or program is deemed more serious than basic hacking.

[856] Assada Endeshaw, 'Computer Misuse Law in Singapore', *Information and Communication Technology*, vol. 8 1(1999): 5-33, p. 14.

[857] Section 3(2) of the SCMA 2013; *cf* section 5(2).

computer virus online, and a victim downloads this virus without any knowledge of its nature and installs it on his computer. The virus then infects the victim's computer and modifies the data or system on it where no hacking was committed. [858] Even for the situation where these two sections indeed both apply, Lee Gen-Min believes it is for judicial convenience:

> 'the availability of the two provisions to deal with that single occasion of misconduct would simply give prosecution a choice of alternative charges to bring against the offender, and that could be determined by considering which offence was easier to prove under the circumstances.'[859]

Section 7 criminalises behaviour that interferes with the use of a computer, or impeding or preventing access to any program or data stored in a computer, namely, obstructing the use of computer.[860] Some scholars point out that section 7 is overlapped with section 5 to some extent.[861] At the first sight, this argument holds true, especially when the modification ruled in section 5 obstructs the use of a computer. However, on a closer scrutiny, these two offences are different. Section 5 protects the integrity of the computer materials by outlawing unauthorised modification of data, yet section 7 protects the availability of computers. Nonetheless, this distinction is not always clear, as illustrated by the scenario of obstructing a system through modifying it.[862]

6.3.1.3 Misuse of devices

Section 8 of the SCMA 2013 mainly introduces criminal offences for those hackers who publish passwords after obtaining them.[863] However, as suggested by Mahalingan and Williams, section 8 is in fact wider than that: it can also be used to criminalise those professionals. To give an example, an author of a book that delivering the weakness of certain systems by illustrating the way this system could be hacked would fall within the ambit of

---

[858] Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, p. 296.

[859] *Ibid*.

[860] Section 7 of the SCMA 2013.

[861] See e.g. Indira Mahalingam and Katherine S. Williams, 'A Step Too Far in Controlling Computers? The Singapore Computer Misuse (Amendment) Act 1998', *International Journal of Law and Information Technology*, vol. 8 1(2000): 48-64, p. 53. The author argues that if a virus obstructed a computer system through modifying its system, it falls within the scope of both s. 5 and s. 7.

[862] Indira Mahalingam and Katherine S. Williams, 'A Step Too Far in Controlling Computers? The Singapore Computer Misuse (Amendment) Act 1998', *International Journal of Law and Information Technology*, vol. 8 1(2000): 48-64, pp. 52-53.

[863] Section 8 of the SCMA 2013.

this provision, if other criteria set in section 8(a), (b) or (c) are met.[864] Ho Tat Kin, specialising in the education business and digital media technology, also pointed out this issue when discussing the Computer Misuse Bill 1993 in the Parliament. He suggested that considering the publication of many computer security articles that openly discuss how to break into a computer system, whether the writers would be assumed to be criminal offenders, was a thorny issue.[865] The then Minister of Home Affairs did not give a clear answer; rather, he replied that

> 'I think it very much depends on the nature of the case. In some cases, it could very well be that the Police can make a case out, in that particular set of circumstance.'[866]

On this issue, the defence mentioned previously – 'in good faith' – may apply. If the actor does such act to educate students or to test the security of a system rather than for immoral intentions, the actor may not be regarded as violated the criminal law.

6.3.1.4 Unauthorised use or interception of computer service

Being regarded as an instrument to penalise online eavesdropping,[867] section 6 contains three different forms that unauthorised use or interception of computer service. These three forms are introduced as three offences in one of the legislative sources of the SCMA – section 342.1 of the Canadian Criminal Code.[868] These three forms are: (1) securing access to a computer to obtain a computer service without authority), (2) intercepting functions of a computer without authority, and (3) using a computer or other device to commit the above two offences.[869]

(1) Securing access to a computer to obtain computer services without authority

Subsection 6(1)(a) criminalises those who 'knowingly secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service'. It is a

---

[864] Indira Mahalingam and Katherine S. Williams, 'A Step Too Far in Controlling Computers? The Singapore Computer Misuse (Amendment) Act 1998', *International Journal of Law and Information Technology*, vol. 8 1(2000): 48-64, pp. 53-54.

[865] *Parliamentary Debates, Singapore Official Reports*, 28 May 1993, cols. 310-311.

[866] *Ibid*, cols. 318.

[867] See e.g. Katherine S. Williams and Indira Mahalingam Carr, 'The Singapore Computer Misuse Act – Better Protection for the Victims?' *Journal of Law and Information Science*, vol. 5 2(1994): 210-226, p. 214.

[868] Amended by clause 45 of the Criminal Law Amendment Act 1985.

[869] Section 6 of the SCMA 2013.

copy of subsection 342.1(1)(a) of the Canadian Criminal Code. In the Canadian context, 'computer service' means 'data processing and the storage or retrieval of data'.[870] In Singapore context, 'computer service' includes 'computer time, data processing and the storage or retrieval of data'.[871] Comparing these two definitions one can notice that the only difference between this subsection and the Canadian equivalent is the inclusion of 'computer time', which literally is not included in the Canadian definition, yet in essence is the computer's capability. Therefore, section 6(1)(a) applies the same approach as adopted by section 342.1 of the Canadian Criminal Code.

However, the approach of the Canadian Criminal Code is different from the one taken by the ECMA, and thus the approach of subsection 6(1)(a) is different from the one of sections 3,4 and 5. This further result in a phenomenon that both section 3 and subsection 6(1)(a) apply to basic hackings, thus makes subsection 6(1)(a) redundant. It is stated under subsection 342.1(1) of the Canadian Criminal Code that fraudulently and without authorisation, obtaining, directly or indirectly, any computer service shall be punished.[872] In this regard, this provision aims at prohibiting acts use computer capability without right. Therefore, it is clear that although performing the same function as what section 3 of the SCMA and section 1 of the England Computer Misuse Act do, the Canadian provision adopts a different approach to criminalising hacking - an approach that focuses on a computer's capability to process and store data.[873] On the contrary, section 3 focuses on the data stored on the computer, and it prohibits unauthorised access or change to the data.[874] Under this approach, the utility or value of a computer is not material for constituting an offence under section 3. Therefore, although judging hacking from different perspectives, subsection 6(1)(a) and section 3 of the SCMA are indeed repetitious.

(2) Intercepting functions of a computer without authority (computer eavesdropping)

Subsection 6(1)(b) criminalises those who 'knowingly intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an

[870] Section 342.1 (Additional Information) of the Canadian Criminal Code 2014.

[871] Section 2(1) of the SCMA 2013.

[872] Section 342.1(1) of the Canadian Criminal Code 2014.

[873] See Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, pp. 48-100. See also Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, p. 304.

[874] Jonathan Clough, 'Data Theft? Cybercrime and the Increasing Criminalisation of Access to Data', *Criminal Law Forum*, 22(2011): 145-170, pp. 153-155.

electro-magnetic, acoustic, mechanical or other device'. Since there is no provision in the England Computer Misuse Act dealing with computer eavesdropping, section 6(1)(b) is deemed by some people as a great improvement on the England Act,[875] to protect the use of computer.

However, this subsection is criticised as being overlapped with sections 3 and 5 under certain circumstances. For instance, the act of taping communications stored on a computer through hacking into it, and instaling malicious software, can easily fall within the ambit of both subsection 6(1)(b) and section 3. What makes the situation more complicated is that since the actor installs malicious software, he may also violate section 5 by modifying the contents of a computer without authority.[876] This kind of overlaps may be commented as bad legislation. On the contrary, some scholars hold a positive attitude towards the overlap. For instance, Gregor Urbas argued that although there is some overlap between this section and other sections, it provides an alternative prosecution for cyber offences.[877]

(3) Using a computer or other device to commit the above two offences

Subsection 6(1)(c) penalises those who 'knowingly uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (*a*) or (*b*)'. Due to adopting another approach, subsection 6(1)(c) leads to the question of what the wording 'using a computer' means, since in sections 3 and 4 the equivalent expression is 'causing a computer to perform any function'.[878] The SCMA itself does not define 'using a computer'. The most relevant interpretation in the SCMA is that the behaviour 'using' constitutes 'causing a computer to perform any function' – the *actus reus* of 'access' to the contents of a computer. Judging from this explanation, this subsection overlaps with section 3 of the SCMA, the access offence, under certain circumstances, since it also criminalises behaviours that access to a computer to commit hacking.

---

[875] Katherine S. Williams and Indira Mahalingam Carr, 'The Singapore Computer Misuse Act – Better Protection for the Victims?' *Journal of Law and Information Science*, vol. 5 2(1994): 210-226, p. 215.

[876] Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, p. 308.

[877] Gregor Urbas, 'An Overview of Cybercrime Legislation and Cases in Singapore', *Asian Law Institute Working Paper Series No. 001*, December 2008, p. 4.

[878] Section 6(1)(c) of the SCMA 2013; *cf* section 3(1) and section 4(1). See Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, p. 312.

Some would argue that this subsection covers attempts at committing offences under subsections 6(1)(a) and (b). For instance, an offender intendis to hack into a computer and install malicious software to tape communications made through a computer. Even so, section 6(1)(c) would still be redundant to some degree considering that if he succeeded section 4 can apply. And if he failed, there is a general provision section 7 classifying attempts as offences.[879]

Generally speaking, the SCMA takes two approaches criminalising cyber wrongdoings: data under sections 3-5 and computer service under sections 6 and 7. As have mentioned previously, the adoption of two approaches results in overlaps and repeat. In addition, according to the definition of 'computer service', 'computer service' contains data storage. However, data storage is far from the security of data. To be specific, under certain occasions although data storage function of computer is not impaired, the security, or in another word, confidentiality, of data stored on that computer is damaged, such as mere hacking under section 3. In this regard, these two approaches do not necessarily contradict or overlap: they can be complementary, and serve to protect the function of computer, and the security of data at the same time. However, Singapore mismatches these two legislative approaches and the acts they prohibit.

6.3.2 Traditional crimes facilitated by computers

6.3.2.1 Computer facilitated fraud and forgery

The SCMA does not introduce any offence regarding computer-facilitated fraud or forgery. Therefore, the first solution is to explore whether the provisions on ordinary fraud and forgery in the Penal Code apply.

Section 415 of the Penal Code rules that 'who induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property' shall be pursued for criminal liability. Before applying this provision to the cyber context, one issue must be addressed, as other jurisdictions have done: whether the stolen or accessed digital information constitutes 'property'. However, a definition or explanation of 'property' is missing in the Singapore Penal Code, and the most relevant definition is 'movable property', which is 'corporeal property of every description, except land and things attached to the earth,

[879] Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, p. 313.

or permanently fastened to anything which is attached to the earth'.[880] Although not pointed out clearly, this definition indicates that 'property' for the purpose of the Penal Code should be material and tangible. In addition, the new promulgated Personal Data Protection Act 2012 defines 'evaluative purpose' as 'for the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property'.[881] This definition also indicates the tangible nature of 'property' in the criminal law context. Therefore, since data is intangible, it cannot be 'property', and section 415 is not applicable to computer-facilitated fraud.

Neither sections under the SCMA nor sections of the Penal Code apply directly to computer-facilitated fraud. In this background, the courts can only apply section 4 of the SCMA to hacking act, and relevant sections of the Penal Code to the further behaviour, such as section 379, the one against theft. The case *Public Prosecutor v. Law Aik Meng* demonstrates this route. Coming from Malaysia, the respondent was part of an organised syndicate. He planted skimming devices comprising data capturing card readers at ATMs, and the card readers captured the card information of its holder, including Personal Identification Numbers (PINs). The device then sent the information to an MP4 player nearby wirelessly. The respondent and his accomplices used the information and cloned bankcards to withdraw cash from ATMs.[882]

When deciding this case, the judges stated that it is inappropriate to apply 'general laws' in cyber context. They explained that

> 'Presently, computer or computer-assisted crimes reported to the Police are dealt with under our general existing laws, e.g. as cases of mischief, theft, cheating, criminal breach of trust under the Penal Code. But it is difficult to proceed under these general laws because of the special nature of computer technology. Furthermore, *the existing penalties under the general laws do not always sufficiently deter computer criminals* … [emphasis added].'[883]

By arguing this, the court insisted that the policy considerations behind the enactment of the SCMA must be taken into account and therefore section 4 of the SCMA applied, together

[880] Section 22 of the Singapore Penal Code 2008.

[881] Section 2 of the Singapore Personal Data Protection Act 2012.

[882] *Public Prosecutor v. Law Aik Meng* [2007] 2 SLR 814; [2007] SGHC 33.

[883] *Ibid.*

with section 379 of the SPC. In other words, the offender firstly violated the SCMA because he secured access to a computer or program with the intention of committing further crimes, and then violated the Penal Code by withdrawing cash from ATMs.[884]

6.3.2.2 Offences related to child-pornography

Like computer related fraud, there are no specific provisions dealing with child-pornography either in the SCMA or in the Penal Code. The provisions apply to producing, selling or distributing child pornography are sections 11 and 12 of the Singapore Undesirable Publications Act, which prohibits acts 'knowingly making, importing, possessing, selling or distributing obscene material and objectionable publications'. 'Obscene material' is the material that 'tends to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it'.[885] 'Objectionable material' refers to the material that 'describes, depicts, expresses or otherwise' deals with

> '(a) matters such as sex, horror, crime, cruelty, violence or the consumption of drugs or other intoxicating substances in such a manner that the availability of the publication is likely to be injurious to the public good; or
>
> (b) matters of race or religion in such a manner that the availability of the publication is likely to cause feelings of enmity, hatred, ill-will or hostility between different racial or religious groups'.[886]

The explanations of obscene and objectionable material are broad enough to include all unwanted acts, therefore, the SUPA is characterised as all encompassing.[887]

Since the SUPA protects publications, the key issue before applying this Act in cyber context is whether postings on the Internet can be regarded as publications. To give a response to this

---

[884] See Gabriela Kennedy and Sarah Doyle, 'A Snapshot of Legal Developments and Industry Issues Relevant to Information Technology, Media and Telecommunications Law in Key Jurisdictions Across the Asia Pacific – Coordinated by Lovells and Contributed to by Other Leading Law Firms in the Region', *Computer Law and Security Report*, 23(2007): 322-331, pp. 324-325. It should be noted that an issue could be raised as to whether an ATM can be deceived: if yes, the offender committed fraud, and if no, he committed theft. In the judgement the court did not give much attention to this point, therefore this issue was beyond the discussion of this part.

[885] Section 3 of the SUPA 1998.

[886] Section 4 of the SUPA 1998.

[887] See e.g. Daniel Seng, 'Regulation of the Interactive Digital Media Industry in Singapore', in Daniel Seng, *Copyright law, digital content and the Internet in the Asia-Pacific*, Sydney: Sydney University Press, 2008, p. 68.

issue, the legislators update the term 'publications' from its traditional version to a cyber version. To date, 'publications' include *'written and printed materials, and by using a computer the information that can be reproduced or shown as any picture, word, statement, sign or representation',*[888] thus wide enough to encompass digital materials. Through doing this, the SUPA applies to cyber wrongdoings relating to child-pornography. This broad definition implies that, as pointed out by the former Minister of Information and the Arts GeorgeYeo, legislators intend to place all Internet transmissions under control for public interest.[889]

Apart from the SUPA, there are several other statutes dealing with obscene or unwanted materials. For instance, under the Films Act,[890] any person who possesses, exhibits or distributes, or reproduces any uncensored (mainly *obscene or lewd)* films is guilty of an offence.[891] Under the Judicial Proceedings (Regulation of Publication) Act, whoever 'prints or publishes in relation to any judicial proceedings any indecent matter or others that would be calculated to injure public morals' shall be punished.[892]

6.3.2.3 Offences related to infringements of copyright and related rights

Computer related copyright infringements are mainly dealt with under the Copyright Act.[893] This Act was amended by the Copyright (Amendment) Act 2004, which introduces the so-called 'primary copyright infringement offence'[894] to regulate computer related copyright

[888] Section 2 of the SUPA 1998.

[889] Daniel Seng, 'Regulation of the Interactive Digital Media Industry in Singapore', in Daniel Seng, *Copyright law, digital content and the Internet in the Asia-Pacific*, Sydney: Sydney University Press, 2008, p. 68.

[890] Singapore Films Act (Chapter 107) 1998.

[891] Section 21 of the Singapore Films Act 1998.

[892] Section 2 and 3 of the Singapore Judicial Proceedings (Regulation of Publication) Act 2013. See also, Michael Hor and Collin Seah, 'Selected Issues in the Freedom of Speech and Expression in Singapore', *Singapore Law Review*, 12(1991): 296-339, p. 325.

[893] Cheng Lim Saw and Susanna H.S. Leong, 'Criminalising Primary Copyright Infringement in Singapore: Who Are the Real Online Culprits', in Cheng Lim Saw and Susanna H.S. Leong, *Copyright law, digital content and the Internet in the Asia-Pacific*, Sydney: Sydney University Press, 2008, pp. 336-338.

[894] The Singapore Copyright (Amendment) Act 2004. It should be noted that there is no definition of primary copyright infringement or secondary copyright infringement. Since it is written in the Copyright Act that the England Copyright, Designs and Patents Act is one of its legislative sources, this part will adopt definitions provided in the England Act. According to Chapter II of the England Act, secondary infringement of copyright includes importing, possessing or dealing with, providing means for making infringing copy, and permitting use of premises for and provision of apparatus for infringing copyright. Though not defining primary infringement of copyright directly, it is indicated in this Chapter that acts including infringement of copyright by copying, infringement by issue of copies to the public, by rental or lending of work to the public, by performance, showing or playing of work in public, by communication to the public and by making adaption or act done in relation to adaption constitute primary infringement of copyright.

infringement. Namely, under section 136(3A), whoever 'produces or deals with music recordings, videos and films, or computer software without right' shall be punished. Especially, if someone conducts 'wilfully copyright infringement where the extent of the infringement is significant or the person does the act to obtain a commercial advantage', a criminal liability shall be pursued.[895]

Prior to this Amendment, 'criminal prosecutions could only be initiated against secondary infringers of copyright (e.g. copyright pirates who commercially exploit infringing copies of copyright material by offering them for sale to the public)'.[896] However, the advances in information technology provide copyright infringers with more opportunities to infringe the intellectual property, for instance, uploading a piece of mp3 to share with others. This phenomenon is referred to as primary infringement of copyright, and there was a need for the legislative response. The Amendment 2004 is the response.

Apart from section 136(3A) of the Copyright Act, section 4 of the SCMA can also apply to copyright infringements, if an offence involves 'property, fraud or dishonesty' under subsection4 (2) and is punishable under the Copyright Act by two years detention or more.[897]

6.3.3 Jurisdiction

Similar to England, Singapore chooses to attach *territorial* principle to the SCMA. Since this principle was established, there has been no substantial change to it. However, this principle is pointed out to have an extra-territorial effect.[898] The extra-territorial effect, according to section 11(1), means an offence wherever is committed, outside or inside Singapore, and whatever the offender's nationality or citizenship is, nonetheless falls within the scope of the SCMA.[899]

---

[895] Section 136 (3A) of the Singapore Copyright Act 2006.

[896] Cheng Lim Saw and Winston T.H. Koh, 'Does P2P have a Future? Perspectives from Singapore', *International Journal of Law and Information Technology*, vol. 13 3 (2005): 413-436, p. 425.

[897] Gregor Urbas, 'An Overview of Cybercrime Legislation and Cases in Singapore', *Asian Law Institute Working Paper Series No. 001*, December 2008, pp. 8 and 19.

[898] Susan W. Brenner and Bert-Jaap Koops, 'Approaches to Cybercrime Jurisdiction', *Journal of High Technology Law*, vol. IV 1(2004): 1-46, pp. 20-21.

[899] Section 11 of the SCMA 2013. The extra-territorial jurisdiction is in fact not a feature shared by the SCMA alone; some other Singaporean statutes also establish the extra-territorial jurisdiction, including *the Misuse of Drugs Act* (Cap. 185), *the Prevention of Corruption Act* (Cap. 241), and several pieces of legislation on protecting vulnerable victims from exploitation. See Kumaralingam Amirthalingam, 'Protection of victims, particularly women and children, against domestic violence, sexual offences and human trafficking', *Asean Law Association*, available at

Subsections 11(2) and (3) may be read as a restriction to this broad range, as only if the offender, the computer, program or data related to the crime was in Singapore at the material time would the SCMA apply.[900] However, the meaning of the term 'material time' is unclear in the Singaporean context. Does it mean the time of the offence occurs? Or the time of investigation starts? Or the time of the prosecution starts? Provided that this section is borrowed from the ECMA, the meaning of 'material time' should be explored in the English context first. According to section 5(2) of the ECMA, the 'material time' refers to 'at the time when [the offender] did the act which caused the computer to perform the function'.[901]

Although with this limitation, the jurisdiction still seems broad. For instance, at the time of the unauthorised act caused a computer to perform some function, the actor was in Singapore, yet the consequence happened in the US. According to section 11 of the SCMA, Singapore has jurisdiction over this case. However, can the Singapore apply jurisdiction since the consequence happened in the US? And if it can, on what occasions can it apply jurisdiction on cases happened in other countries? To answer these questions, a scholar argues that before Singapore applies the jurisdiction, three factors must be observed:

> 'there should be a substantial and bona fide connection between the subject-matter and the source of the jurisdiction;
>
> the principle of non-intervention in the domestic or territorial jurisdiction of other states should be observed;
>
> that a principle based on elements of accommodation, mutuality and proportionality should be applied. Thus nationals resident abroad should not be constrained to violate the law of the place of residence'.[902]

With these factors, it is not surprising that although Singapore has attached an extraterritorial effect, the jurisdiction has rarely been invoked. For instance, in the case *Public Prosecutor v. Taw Cheng Kong,*[903] the Court of Appeal refused to apply the jurisdiction by arguing that:

---

http://webcache.googleusercontent.com/search?q=cache:8LoNORqD91MJ:www.aseanlawassociation.org/9GAdocs/w5_Singapore.pdf+andcd=1andhl=zh-CNandct=clnkandgl=nlandclient=firefox-a. Last visited November 2014.

[900] Section 11 of the SCMA 2013.

[901] Section 5(2) of the Engalnd Computer Misuse Act.

[902] Ian Brownlie, *Principles of Public International Law* (6th edition), Oxford: Oxford University Press, 2003, p. 309.

> 'referring therein to an explicit non-application to foreigners clause in an extraterritorial statutory provision, went on to consider international comity and international law as reasons for the non-application of the statute to foreigners, and thus as reasons for saying that non-application of the statutory crime therein to a particular class of persons would not occasion a violation of the equal protection clause in the Singapore Constitution.'[904]

Since the extra-territorial jurisdiction has rarely been invoked, some scholars maintain that such a broad extraterritorial effect is nothing but a deterrent, and 'when the occasion arises, [it] affords a mechanism for doing justice'.[905] As Dr. Toh Keng Kiat put it:

> '…I doubt that when the audit trail of a computer misdeed, particularly one that deals with security matters, leads to such a teenage hacker, we will be prepared to surrender him to a foreign country for prosecution, extradition and mutual assistance arrangement notwithstanding. Vice versa, I doubt that a foreign country will also readily give up one of its citizens for trial here for a similar offence.'[906]

As a summary, it can be noticed that although Singapore attaches the extra-territorial effect to its jurisdiction principle, in fact its jurisdiction is a paper tiger. Before releasing this tiger, many issues need to be considered and many factors need to be balanced, such as the judicial sovereignty of other countries.

6.4 The Scope of Cybercrime and the Enforcement Measures

This section focuses on two topics, namely, the scope of cybercrime in Singapore and the enforcement measures the SCMA grants to the officials. The extent to which the term of 'cybercrime' should reach and be regulated has always been a hot topic. The English, Canadian and American cybercrime legislations have great influence on the SCMA. The attitudes on the scope of cybercrime in these three jurisdictions also have significant influence on Singaporean scholars. Besides, it can be seen from the historical review of the SCMA that the enforcement measures granted to officials keep expanding. It seems the argument on the

---

[903] *Public Prosecutor v. Taw Cheng Kong* [1998] 2 SLR 410. To be noted that this case was brought for trial under the Prevention of Corruption Act.

[904] C. L. Lim, 'Singapore Crimes Abroad', *Singapore Journal of Legal Studies*, (2001): 494-536, p. 495.

[905] Kumaralingam Amirthalingam, 'Protection of Victims, Particularly Women and Children, against Domestic Violence, Sexual Offences and Human Trafficking', *Asian Law Association*.

[906] *Parliamentary Debates, Singapore Official Reports*, 28 May 1993, cols. 314.

potential abuse of powers and the consequent infringements of online freedom do not get sufficient attention. Therefore, 6.4.2 shed lights on this issue, intending to investigate how Singapore strikes the balance between online freedom and the control over cyberspace.

6.4.1 The scope of cybercrime

Before discussing the scope of cybercrime in Singapore, one important topic is the scope, or the definition, of 'computer'.

In the SCMA 1993, the term 'computer' under section 2(1) was defined as

> 'an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, a portable hand-held calculator or other similar device which is non-programmable or which does not contain any data storage facility'.

According to scholars, on the one hand, this definition was 'sufficiently wide and exclusive to protect technology that may appear afterwards', and 'sufficiently clear to avoid questions of whether a hand-held calculator falls within the reach of the Act or not' at the same time.[907] On the other hand, it was commented by others as being clumsily worded and ambiguous.[908] For instance, it was not clear whether or not tampering with chips inside 'non-programmable'

[907] See e.g. Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, pp. 267-268. In this article the author argues that 'but does not include' indicated that certain devices were not considered sufficiently computer-like and that they fell outside the Act. He then further pointed out that any other data processing devices that did not fall in the exclusion list were likely to be a computer under the SCMA 1993.

[908] See e.g. Indira Mahalingam and Katherine S. Williams, 'A Step Too Far in Controlling Computers? The Singapore Computer Misuse (Amendment) Act 1998', *International Journal of Law and Information Technology*, vol. 8 1(2000): 48-64, p. 49. See also Katherine S. Williams and Indira Mahalingam Carr, 'The Singapore Computer Misuse Act – Better Protection for the Victims?' *Journal of Law and Information Science*, vol. 5 2(1994): 210-226, p. 212. This article argues that the wording 'other data processing device' could be applied to a device that using biological memory which might occur after the SCMA 1993.

devices was covered,[909] and neither was whether household devices such as washing machines with storage and computing capability were covered.[910]

Therefore, the Evidence (Amendment) Act 1996 amended the definition of 'computer'. The new definition, as suggested previously, grants the government the power to list out devices that they do not recognise as computer. Although being criticised as 'a novel extension for administrative convenience',[911] this definition was still affirmed in the SCMAA 1998, and applies till now.

Since there has already been a definition on 'computer', one may assume that a consensus on the definition of 'cybercrime' may not be hard to reach. Is this true? The answer is negative. Moreover, scholars in Singapore reach a consensus that the definition of cybercrime or computer crime is in fact not clear,[912] so as to its scope. Mainly there are three different opinions on the definition of computer crime/cybercrime.

Firstly, to some scholars, the terms 'computer crime' and 'cybercrime' are different. For instance, Warren B. Chik believes that 'computer crime' refers to crimes 'committed against the computer, the materials contained therein such as software and data, and its uses as a processing tool', including 'hacking, denial of service attacks, unauthorised use of services and cyber vandalism'; while cybercrime means 'criminal activities committed through the use of electronic communications media', including 'cyber-fraud and identity theft through such methods as phishing, pharming, spoofing and through the abuse of online surveillance technology'.[913] There is another distinction between computer crime and cybercrime. That is, whether is covered by the existing criminal law. For instance, scholars such as Douglas H. Hancock suggest that offences under the SCMA are computer crimes, and offences under the existing laws are cybercrime. To be clearer, computer crimes are generally new and

[909] Assafa Endeshaw, 'Computer Misuse Law in Singapore', *Information and Communications Technology Law*, vol. 8 1(1999): 5-33, p. 8.

[910] See e.g. Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331, pp. 267-268.

[911] Indira Mahalingam and Katherine S. Williams, 'A Step Too Far in Controlling Computers? The Singapore Computer Misuse (Amendment) Act 1998', *International Journal of Law and Information Technology*, vol. 8 1(2000): 48-64, p. 50.

[912] See e.g. Terry Johal, 'Controlling the Internet: The Use of Legislation and Its Effectiveness in Singapore', in *15th Biennial Conference of the Asian Studies Association of Australia*, Canberra, 2004.

[913] Warren B. Chik, 'Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore', available on www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc/. Last visited September 2014.

technology-specific, and they threaten the integrity, availability and confidentiality of the computer, data, and programs stored on the computer. Therefore, they need a new and specialised statute. On the contrary, cybercrimes are merely old crimes committed with new means, and thus fall within the regime of the existing laws.[914]

Secondly, some scholars acknowledge that computer crime and cybercrime are different, and the term 'computer crime' is more appropriate. However, to what acts these two terms are referring is unclear. These scholars do not and cannot define them. By citing the words of Colin Tapper, an English scholar, they express their confusion: 'does the phrase connote crimes directed at computers, or crimes utilising computers, or merely crimes in any way at all related to computers?'[915] To this question, Colin himself states that computer (related) crime is 'so inherently vague as a concept.'[916]

Thirdly, more scholars tend to regard computer crime and cybercrime as the same, as several other jurisdictions do. This group of scholars define computer crime as 'criminal activities against a computer or facilitated by or committed by the use of a computer'.[917] However, they admit that this definition is still unclear with respect to crimes facilitated by or committed by the use of a computer. They cannot reach a consensus on the issue that to what extent the phrases 'facilitated by' and 'by the use of' should reach.

From a statutory perspective, computer crime in Singapore includes mere hacking, hacking to facilitate further crimes, unauthorised modification and obstruction of computer data or system, and trafficking passwords or publishing other means of hacking, i.e. the genuine cybercrime.

6.4.2 The enforcement measures under the Computer Misuse Act

The SCMA has taken a positive attitude on granting officials powers. Starting from 1993, section 14(a)[918] empowered the Police officer to 'demand access to and inspect or check the operation of any computer, and any associated apparatus or material which he has reasonable

[914] *Ibid.* See also Douglas H. Hancock, 'To What Extent Should Computer Related Crime be the Subject of Specific Legislative Attention?' *Albany Law Journal of Science and Technology*, 12(2001): 97-124.

[915] Colin Tapper, 'Computer Crime: Scotch Mist?' *Criminal Law Review*, (1987): 4-22.

[916] *Ibid*, p. 6.

[917] See e.g. Na Jin-Choen, Wu Hao, Ji Yong, Tay Mia Hao, and Ramanathan Mani Kandan, 'Analysis of Computer Crime in Singapore using Local English Newspapers', *Singapore Journal of Library and Information Management*, vol. 38 (2009): 77-102, p. 78.

[918] Section 14 becomes section 15 in the SCMA (1998 revised).

cause to suspect is or has been in use in connection with any offence under the Act', and section 14(b) entitled the Police to require the suspect to provide them with reasonable assistance for the purpose of subsection (a). Because the evidence gained through required acts may be used against the suspect in the later prosecution or trial, this section actually amounts to self-incrimination, which directly contradicts the international standards of individual rights.[919] This power granted to the Police was criticised for its:

> 'lack of safeguards (in the form of approval from independent third parties) to check abuse,
>
> infringement of the rights to privacy, and
>
> infringement of the right against self-incrimination'.[920]

In 1998, to provide a restriction on the investigative power under the SCMA, legislators replaced section 14 with a new one. However, the new section did not truly restrict the power. Admittedly, the new section 14 required the police officer to obtain permission from the Public Prosecutor before he took measures, for instance, 'requiring any person in possession of decryption information to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence'.[921] This requirement was limited to section 14 (1)(a)(ii) and (iii) and 14 (c). In other words, no consent from the Public Prosecution was obligatory for the Police to wave the power granted by section 14(1)(a)(i) - having access to and inspecting and checking the operation of any computer to which this section applied. This legislative omission is commented as odd, and 'no justification came easily to mind'.[922]

Five years later, the SCMAA 2003 inserted section 15A under section 15, entitling the Minister to empower any person or organisation to take necessary measures to prevent or counter any threat to a computer system, which can affect the national security, essential

---

[919] Sections 14 and 17 of the International Covenant on Civil and Political Rights (ICCPR).

[920] Indira Mahalingam and Katherine S. Williams, 'A Step Too Far in Controlling Computers? The Singapore Computer Misuse (Amendment) Act 1998', *International Journal of Law and Information Technology*, vol. 8 1(2000): 48-64, pp. 60-61.

[921] Section 14(c) of the SCMA 1998.

[922] Indira Mahalingam and Katherine S. Williams, 'A Step Too Far in Controlling Computers? The Singapore Computer Misuse (Amendment) Act 1998', *International Journal of Law and Information Technology*, vol. 8 1(2000): 48-64, p. 61.

services, defence or foreign relations of Singapore.[923] Towards this expansion of enforcement powers, questions were raised during the Parliamentary debate. The raised questions were mainly concerning one issue: the margin between respecting individual rights of ordinary people and preventing a terrorist attack on critical networks. For the one, Mr M. Ravindran, a lawyer specialising in trademark law, expressed his concern about how to ensure adequate safeguards to protect the privacy of law-abiding citizens;[924] for another, the extensive power granted to the Police worried the speakers for its potential abuses. As an example, associate professor Chin Tet Yung asked:

> 'the powers conferred in the original section 15 are extremely wide. What, may I ask, are the additional powers (under section 15A) that are contemplated which are not within section 15?'[925]

In response to this, the then Senior Minister of State, Ministry of Home Affairs, associate professor Ho Peng Kee, explained that the focuses of these two provisions were different:

> 'This [section 15] is more the traditional approach to crime solving. Moreover, the powers are limited as they can only be applied to a computer that is reasonably suspected or has been used in connection with an offence under the Act or any other criminal offence. Hence…I am sure Prof. Chin will agree by now, the existing powers that we have, both under the Computer Misuse Act and also other legislation, are definitely inadequate to deal with cyber threats against out national interests. That is why we need this new section…And as I have mentioned earlier, many other countries have, in fact, enacted laws which are similar to and, indeed, some wider than ours…We need a wide approach because it is necessary to take pre-emptive steps…there must be grounds to believe that such systems, if attacked successfully, would result in a disruption of Singapore's critical infrastructure and essential services.'[926]

He also emphasised the necessity of section 15A by stating that measures under section 15 were not enough:

---

[923] *Parliamentary Debates, Singapore Official Reports*, 10 November 2003, Introduction.

[924] *Ibid*, cols. 3329.

[925] *Ibid*, cols. 3327.

[926] *Ibid*, cols. 3334 and 3335.

> 'As they [the measures under section 15] focus primarily on dealing with a cyber-attack after it has happened. We need to empower our security agencies to take pre-emptive steps to prevent a cyber-attack on our systems because once it happens, the consequences are dire.'[927]

In addition, the proposal of section 15A can also be explained by the widely used 'preventive detention'[928] in a non-cyber context with the aim of preventing harm from happening.[929] Applying this aim to the cyber context, the proposed pre-emptive measures seem reasonable.

During the Second Reading of the proposal of section 15A, Parliament members raised the issue concerning the potential infringement of human rights. However, none of them voted against this proposal because of the concern over Singapore's national interests.[930]

The amendments enacted in 2013 have followed the extending trend of enforcement powers. The powers granted by the SCMAA 2013 are (1) if a person fails to take measures or does not comply with the directions of the Minister or someone who is acting pursuant to a certificate issued by the Minister, he would thus be pursued for criminal liability; (2) various immunities are established for acts done in good faith pursuant to the Minister's certificate to ensure that those who are acting pursuant to the certificate or direction can perform their functions without being constrained for fear of civil or criminal liabilities.[931]

When discussing the Amendment 2013, the Second Minister of Home Affairs, Mr S. Iswaran, again, stated that the powers under section 15A were no longer sufficient. He introduced a term 'Critical Information Infrastructure' (hereafter the CII), and emphasised the potential damage of computer misuse to the CII.[932] He further stated that given the rapid development in technology and sophistication of saboteurs an amended and enhanced section 15A was

---

[927] *Ibid*, cols. 3324.

[928] Section 8, Chapter II of the Singapore Internal Security Act, Chapter 143, 1985 Rev. Ed.

[929] Michael Hor, 'Terrorism and The Criminal Law: Singapore's Solution', *Singapore Journal of Legal Studies*, (2002): 30-55, pp. 46-47.

[930] See e.g. *Parliamentary Debates, Singapore Official Reports*, 10 November 2003, cols. 3327.

[931] Section 15A of the SCMA 2013.

[932] CII was referred to as 'systems that are necessary for the delivery of essential services to the public in various key sectors'. *Parliamentary Debate, Singapore Official Report*, 14 January 2013, 3.03 pm.

necessary and would strengthen the security of CII by enabling governmental officers to take more effective and timely measures.[933]

The new 15A empowers officers to disclose information they obtained under the Minister's certificate for cases with respect to national security, essential services or defence of Singapore or the foreign relations of Singapore. As a restriction on this power, information obtained through this way can only be disclosed for the purpose of preventing, detecting or countering the cyber threat, with three exceptions.[934] In addition, the new 15A also extends the meaning of 'essential service', and now it includes 'services directly related to land transport infrastructure, aviation, shipping and health services'.[935]

Still, this time, all the members of the Second Debate supported this Amendment. Similar to the supporting arguments raised in 2003, the considerations expressed by the members were mostly based on national interests,[936] and one of these members even worried that it would take too long for the Amendment 2013 to be passed.[937] Problems regarding the protection of privacy and abuse of power were raised,[938] while for the first the Minister gave assurances that the enhanced powers were not intended to infringe personal privacy, by explaining that the new measures were mainly technical in nature, and for the second she promised a judicious exercise of the powers under section 15A.[939]

Judging from this historical review of the enforcement measures in the SCMA, one can see that between online freedom and control over cyberspace, Singapore has always chosen to enhance the control. The motivation behind this choice, as both have been identified by scholars and emphasised by Parliament members, is national security.

---

933 *Ibid.*

934 For exceptions see section 15A (8) of the SCMA 2013.

935 Section 15A (12) of the SCMA 2013. See also *Parliamentary Debate, Singapore Official Report*, 14 January 2013, 3.03 pm.

936 See e.g. the speeches of Mr Hri Kumar Nair, 3.17 pm and Mr Christopher de Souza, 3.22 pm in the Second reading of the Computer Misuse (Amendment) Bill 2013.

937 The speech of Associate professor Fatimah Lateef, 3.42pm in the Second Reading of the Computer Misuse (Amendment) Bill 2013.

938 See e.g. speeches of Mr Hri Kumar Nair, 3.17 pm and Mr Desmond Lee, 3.35 pm in the Second Reading of the Computer Misuse (Amendment) Bill 2013.

939 *Parliamentary Debate, Singapore Official Report*, 14 January 2013, 4.05 pm.

6.5 Summary

Singapore has been active in promulgating and amending its Computer Misuse Act. The approach it takes is remarkable for the overlaps and repeats within provisions. Firstly, it learned from the England Computer Misuse Act and introduced hacking offences threatening the security of data, including mere hacking, hacking for further crimes, modification of data, and others. At the same time, it borrowed the Canadian equivalent provisions and introduced hacking offences focusing on the computer's processing and storage capability, for instance, using computer services without authority. Secondly, two offences inserted by the SCMAA 1998 are overlapped with previous offences, which make them difficult for judges to apply. Therefore, some scholars stated that the idea behind these overlapped provisions was to ensure the incrimination of computer misuses. For this purpose, Singapore does not distinguish between computer and data. Any offence that violates either computer or data shall be prosecuted. However, as suggested, these two approaches are not necessarily contradictive. As the information technology develops, cybercrime starts to target both the security of data and the function of computers. This development suggests that the adoption of one approach, i.e. protecting either data or computer, may be insufficient. Thus, they two can be complementary.

The other characteristic of the Singaporean approach against cybercrime is its broad enforcement measures. The enforcement measure has been expanded dramatically since its birth, driven by the concern over national security. Admittedly, such expansion can be partly explained by the fact that traditional enforcement measures cannot tackle the newly emerged forms of computer misuse. However, the new forms of computer misuses cannot account for all expansions. The introduced new provisions, the enhanced penalties, the ever-expanding enforcement measures, and the extra-territorial effect attached to the SCMA all indicate Singapore's position on criminalising and deterring computer misuse – to enhance national security, even though such enhancement impairs privacy and online freedom. This ideology can also be illustrated by the fact that it took Singapore more than one decade to pass the Personal Data Protection Act to protect personal information.[940]

One possible reason for this ideology is that Singapore's political culture leads it to deploy Internet technology in ways that reflect concerns for social order and the maintenance of

[940] Gabriela Kennedy, Sarah Doyle and Brenda Lui, 'Data Protection in the Asia-Pacific Region', *Computer Law and Security Review*, vol. 25 (2009): 59-68.

hierarchy.[941] Just as pointed out by Junhao Hong, Singapore uses law more to protect and serve government interests than to protect individual interests because of its similarities in ideological and political structures with China.[942] It is interesting to point out that both in Singapore and China, the use of Internet is deemed to link with democracy and political ideology; the issue of whether information technology can promote democracy in these two jurisdictions, and even in the whole Asian-Pacific region, has been under heated discussion.[943]

[941] Randolph Kliver and Indrajit Banerjee, 'Political Culture, Regulation, and Democratization: The Internet in Nine Asian Nations', *Information, Communication and Society*, vol. 8 1(2005): 30-46, p. 36.

[942] Junhao Hong, 'The Control of the Internet in Chinese Societies: Similarities, Differences, and Implications of the Internet Policies in China, Hong Kong, Taiwan, and Singapore', *Proceedings of the Asia Internet Rights Conference. Seoul, S. Korea,* November 2001.

[943] See e.g. Nina Hachigian, 'The Internet and Power in One-Party East Asian States', *The Washington Quarterly*, vol. 25 3(2002): 41-58. See also Shanthi Kalathil and Taylor C. Boas, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*, Washington D.C.: Carnegie Endowment for International Peace, 2003.

Chapter 7 Comparison, Conclusion and Recommendation

7.1 Introduction

The previous Chapters have investigated and analysed the legislation related to cybercrime in the selected legal regimes, including China, the United States (US), England, Singapore, and the Council of Europe (CoE). This Chapter intends to answer the central research question, i.e. how to adapt the criminal law to regulate cybercrime, by drawing comparative observations and conclusion. Afterward, it proposes recommendations to China.

Firstly, a comparison among the cybercrime legislations and the legislative approaches reflected in the selected legal regimes is provided. This comparison is structured on seven topics generalised from the previous study on individual jurisdictions, especially through identifying the convergences and divergences among the legislations and approaches. In particular, the comparison is made on how these legal regimes strike the subtle balance between online freedom and cybercrime criminalisation and addresses the core contentious issues regarding cybercrime.

Secondly, based on the comparison, the conclusionof this research is presented in accordance with the four aspects of the central research question. These four aspects are

> Aspect 1: the necessity of a cyber-specific legislation;
>
> Aspect 2: the possible and systematic approaches the legislation can take to determine and regulate cybercrime;
>
> Aspect 3: the adequate and sufficient jurisdiction principle over cybercrime; and finally,
>
> Aspect 4: the function and influence of the Convention on Cybercrime in shaping approapriate legislation and fostering international cooperation against cybercrime.

Thirdly, based on the conclusion, recommendations are proposed to China regarding how it can improve its current legislative approach of the criminal law so as to be more effective and adequate in resolving issues that arise from cybercrime.

It should be noted that although the Convention on Cybercrime (CoC) of the CoE is not legislation in the same sense as the domestic legislations of this research, the detailed

provisions against cybercrime it contains make it comparable to national legislations. In addition, the approach behind it provides insights on answering the central research question of this research. Thus, the CoC is also used as a comparison subject under this Chapter.

7.2 Comparison

Having examined the cybercrime legislations and their evolving processes in the selected jurisdictions and the CoE in previous Chapters, this section primarily focuses on the questions the extent to which the legislative approaches taken by the legal regimes resemble each other and how jurisdictions can benefit from each other.

7.2.1 On-going legislative process in expanding cybercrime legislation

Information technology develops rapidly around the world, and so does cyber wrongdoings. To deter cyber wrongdoings, the selected jurisdictions and the CoE introduced cyber-specific criminal offences. However, the newly introduced criminal offences increasingly become insufficient on covering and deterring cyber wrongdoing as it keeps on developing. Therefore, the criminal offences have been reviewed, amended, and expanded.

7.2.1.1 Specific cybercrime Act v. general criminal law

All the five selected legal regimes have promulgated new provisions to deal with cybercrime, as observed in previous Chapters. However, the forms of the provisions differ: as a part of the Criminal Law, or as a specific criminal Act. While China has introduced six Articles concerning cybercrime under Chapter VI of the CL, entitled as the Crimes Obstructing Public Order,[944] the CoE, US, England and Singapore have enacted new and specific criminal Acts concerning cybercrime. The form adopted by China implies that cybercrime is not regarded as a unique and specific category of crime; instead, it exists as a subgroup of crimes that threatening public order. In contrast, the specific Act other selected legal regimes adopt may suggest the special and distinguished treatment of cybercrime. Comparing these two forms one can observe that the choice of either inserting new provisions in the Criminal Law or promulgating specific Act is not material to a substantial degree in judicial practice.

Admittedly, it may be assumed that the form adopted by China may lead to some degree of confusions and overlaps between computer offences and traditional offences. The reason for this assumption is that provisions in the general criminal law may not distinguish computer

[944] Chapter VI of the Criminal Law, China.

crimes from traditional ones, and therefore, confusions may arise on the issue to which situations provisions against traditional crime apply and to which situations provisions against cybercrime apply. On the contrary, a specific Act can better emphasise the involvement of the computer in a crime and the punishable nature of that involvement, and by doing so confusions among provisions can be avoided.

However, facts have shown that on the very issue of avoiding confusions, the specific Act adopted in other selected legal regimes does not necessarily do a better job than the provisions in the general criminal law of China. This argument can be proved through addressing online fraud. Offender A hacks into victim B's computer and obtains B's personal information. By using this information, A tricks B into willingly transferring money to A's account. In a case like this, both of the criminal provisions against fraud (traditional crime) and hacking (cybercrime) may apply. Which provision can apply to such situations is decided by the *actus reas* and the *mens rea* of the activity, but not by the form of the provisions. The Singapore Computer Misuse Act can also be used to prove the argument. A main characteristic of the SCMA, as revealed in the Chapter on Singapore, is the overlaps and repeats among provisions. For instance, section 3 is overlapped substantially with section 6 because both of them are drafted to criminalise unauthorised access. Instead, analysing from the wordings of the cybercrime provisions in the Chinese criminal law, one can hardly notice any substantial overlap or repeat.[945]

In addition, the choice on the form of new and specific provisions is decided not on the consideration of avoiding confusions, but made on the basis of the legal tradition and in a certain historical context. As mentioned already in the Chapter on Singapore, according to the previous Minister for Home Affairs of Singapore, Prof. S. Jayakumar, a computer-specific Act was drafted to send a deterrent signal to those who intend to commit crimes involving the use of computer.[946] In contrast, China chooses to insert new provisions into the CL because it preferred a comprehensive and all-inclusive Criminal Law when revising the CL in 1997. According to Chinese scholars and judges, Chinese legislators had issued 24 specific criminal Acts before 1997 to supplement and amend the then criminal law,[947] and these specific Acts

[945] Indeed there are overlaps and repeats between laws and regulations at different levels, the provisions of the criminal law are not overlapped substantially. For the overlaps and repeats between laws and regulations at different levels, see section 2.2 of Chapter 2.

[946] *Parliamentary Debates, Singapore Official Reports*, 28 May 1993, cols. 300 – 304.

[947] The 24 specific criminal Acts introduced offences such as kidnap, embezzlement and others. They also amended criminal provisions against bribery and corruption, tax evasion, smuggling and others. When the CL

made the application and interpretation of criminal provisions complicated. In this background, Chinese legislators combined the specific Acts and the CL together and created an all-inclusive Criminal Code – the CL 1997.[948] Therefore, provisions with respect to cybercrime were also included as a part of the general Criminal Law.

In sum, a specific Act on cybercrime does not mean a distinguished treatment of cybercrime and traditional crime, and provisions in general criminal law do not mean repeats and overlaps either. As long as the provisions on cybercrime are specific, whether they are in a specific Act or in the criminal law does not matter to a substantial degree.

7.2.1.2 The origin of cybercrime legislation: the inadequacy of traditional criminal provisions and the consequent necessity for new cybercrime legislation

Before enacting new cybercrime legislation, the selected legal regimes had attempted to stretch the traditional criminal laws in cyber context, however found them inadequate. Therefore, all the five selected jurisdictions and the CoE choose to promulgate new legislations tackling cybercrime rather than relying on traditional ones.

The experience accumulated by previous attempts and discussions has been reflected to different degrees in the selected legal regimes. China, the CoE and England, although have different experiences of applying traditional criminal provisions, coincidently distinguish the genuine cybercrime from the traditional crimes facilitated by computers, and introduce new offences on the genuine cybercrime. The US, since the first bill against computer wrongdoing was criticised as too broad, limited the coverage of the Computer Fraud and Abuse Act intentionally. Ironically, the broad scope of this bill was the result of previous attempts, and the intentionally limited scope of the CFAA was soon proved too limited in judicial practice. Singapore did not explicitly attempt to criminalise cybercrime before its SCMA. This to some

---

was revised in 1997, all the 24 specific Acts were combined together with the Criminal Law. After 1997, only one specific Act was issued in 1998, the one against evasion of foreign currency. After this 1998 specific Act, China started to use the Amendment to upate and amend the CL. See Hao Xingwang, '我国单行刑法的若干基本理论问题研析' (An Analysis of the Bsic Theoretical Isusses on the Specific Act), *Faxue Jia* (The Jurist), 4(1994): 39-45. Zhao Yanguang, '十五年刑法补充、修改述要（上）' (Main Amendments and Supplements of the CriminL Law in the Last Fifteen Years (Part I)), *Faxue Pinglun* (Law Review), 4(1994): 6-12. Huang Huaping and Liang Shengyuan, '试论刑法修正案的立法模式' (An Analysis of the Legislative Approaches of the Amendments to the Criminal Law), *Zhongguo Renmin Gongan Daxue Xuebao* (Journal of Chinese People's Public Security University), vol. 115 3(2005): 6-13.

[948] See e.g. Hao Xingwang, '我国单行刑法的若干基本理论问题研析' (An Analysis of the Bsic Theoretical Isusses on the Specific Act), *Faxue Jia* (The Jurist), 4(1994): 39-45. See also Li Yuzhen, '刑法法典化的重大意义' (The Significance of Codification of Criminal Law), *Zhengfa Luntan* (Tribune of Political Science and Law), 3(1997): 8-10.

extent results in the lack of experience of regulating cybercrime, and further results in the absence of a consistent and systematic approach in the cybercrime legislation.

Table 7.1 The promulgating year of the first cybercrime legislations and the subsequent amendments in the selected legal regimes

	First cybercrime legislation	**Later Amendments**
China	1997	2009, 2015
CoE	2001	[949]
US	1984	1986, 1988, 1989, 1990, 1994, 1996, 2001, 2008
England	1990	2006, 2015
Singapore	1993	1996, 1998, 2003, 2013

Chinese legislators maintained that traditional criminal provisions are only applicable to crimes facilitated by computers, and new legislation is necessary on the crimes targeting computers. In China, two issues had been discussed in particular before the enactment of Articles against computer crime. They are (1) whether all computer crimes were the same from the perspective of their target, *mens rea* and *actus reas*, and (2) whether traditional criminal provisions could apply to computer crime. For the first issue, the inclusion of Article 287 implies that not all computer crimes are the same. Offences under Articles 285 and 286 involve the targeting of computers; while offences under Article 287 are those using the computer as a tool to commit traditional crimes. Therefore, crimes facilitated by computers and those targeting computers are distinguished. In other words, the genuine cybercrimes, i.e. crimes under Articles 285 and 286, and the traditional crimes facilitated by computers, acts under Article 287, are distinguished. In addition, within the subgroup of the genuine cybercrime, the acts prohibited under Articles 285 and 286 also differ. Specifically, Article 285 penalises illegal access to computers involved in listed areas; while Article 286 penalises

[949] There is an additional protocol to the Convention on Cybercrime. However, this additional protocol changes neither the text of the CoC nor the approach the CoC takes. Rather, it follows the approach of Arts. 9 and 10 of the CoC, and establishes a subcatogery of offences related to racism. Therefore, this protocol is not regarded as an 'amendment' under this research, and is left out from detailed discussion.

behaviours damaging the function of computers. With respect to the second issue, if the answer was yes, the legislators did not need to draft new criminal provisions. In that case, judge could apply traditional criminal provisions to online fraud and theft for instance. Otherwise, new criminal provisions would be necessary. The inclusion of computer-specific Articles 285 and 286, and the non-specific Article 287 in the CL 1997 indicates the legislators' position as regards this discussion. That is, traditional criminal provisions are not applicable at least to the crimes targeting computers.[950]

The Council of Europe had attempted to treat cybercrime as economic crimes in the beginning, and other traditional crimes in the later period. However, these attempts did not succeed because the legal framework against traditional crimes soon became lack of coverage compared with cybercrime. To be specific, the CoE had begun its attempts of adopting the criminal law to regulate cybercrime in the 1970s. Initially, the experts appointed by the CoE tried to address cybercrime under the framework of the then existing criminal provisions against economic crime.[951] However, this attempt did not succeed because computer crime evolved so quickly that it soon outstripped the concept of economic crime. Then in the 1980s, the Council of Europe decided not to limit computer crimes to the economic crimes, and recommended to apply the then existing criminal provisions to computer crime. This attempt once again did not succeed because computer crime evolved too rapidly and the then existing criminal provisions soon appeared insufficient. Stretching the then criminal provisions into cyber context would raise concerns about analogical interpretation. The CoE thus acknowledged the necessity for special criminal provisions to deal with crimes involving computers, and this acknowledgement led to the launching of many research programmes and seminars on drafting new criminal provisions in the later period.[952] As the result of the research programmes and seminars, the experts appointed by the CoE listed several forms of cybercrime that need to be criminalised, including computer fraud, computer forgery, damage to computer data or programs, computer sabotage, unauthorised access, unauthorised interception, unauthorised reproduction of a protected computer program and unauthorised

[950] For more detailed information on the evolution of criminal provisions regarding cybercrime in China, see Chpater 2 Cybercrime Legislation in China.

[951] For how the Convention was fitted into the framework of economic crime and fraud, see Chapter 3 The Convention on Cybercrime of the Council of Europe.

[952] For more detailed information of these attepmts see Chapter 3 The Convention on Cybercrime of the Council of Europe.

reproduction of a topography.[953] However, in this period the experts did not distinguish between the genuine cybercrime and traditional crime facilitated by computers. This indiscrimination to some extent resulted in the absence of the definition of cybercrime: the mere involvement of computer, or some more technologically specific elements that make a crime a cybercrime. This indiscrimination is changed in the completed Convention on Cybercrime, in which the genuine cybercrime and crimes facilitated by computers are put in different categories. Moreover, the CoC distinguishes between damage to data and damage to computer - the device.[954]

The US started its attempts to criminalise offences with computers involved as early as the 1970s, through applying the then existing criminal provisions. However, it soon realised that the possibility to apply existing criminal provisions to any given activity depended on the chance of particular elements being present in the activity,[955] rather than on whether the activity had caused serious harm. Therefore, it began to draft a computer specific act comprehensive enough to cover all computer misuses. Therefore, the Bill of the Federal Computer Systems Protection Act (BFCSP) was introduced to Congress in 1977, and under it any knowing and wilful manipulation, or attempted manipulation, of a computer (or any part of a computer) for the purpose of defrauding or obtaining money was criminalised.[956] Nonetheless, it was not passed because it was widely criticised for being too broad in scope and infringing online freedom excessively. Considering this criticism, the US legislators intentionally limited the criminalisation scope of the future bills on computer crime. Finally, the Computer Fraud and Abuse Act was passed and enacted in 1984.[957]

In England, the Computer Misuse Act (ECMA)[958] was promulgated in 1990, but the attempts at incriminating computer-involved offences can be traced back to the 1970s, the same period

---

[953] The Council of Europe, Recommendation No. R (89) 9 on Computer-related Crime and Final Report of the European Committee on Crime Problems, *Strasbourg* 1990.

[954] See Chapter 3 The Convention on Cybercrime of the Council of Europe.

[955] As the case *United States v. Seidlitz* shows, if not the offender committed the offence across the state border, traditional provisions could not apply. For more details see Chapter 4 Cybercrime Legislation in the US.

[956] See John Roddy, 'The Federal Computer Systems Protection Act', *Journal of Computers, Technology and Law*, 7(1976): 343-365.

[957] Enacted with the name of *The Counterfeit Access Device and Computer Fraud and Abuse Act*, Pub. L. No. 98-473. Changed to *Computer Fraud and Abuse Act* in 1986.

For more details of the US' attepmts on applying the traditional criminal law see Chapter 4 Cybercrime Legislation in the US.

[958] Considering that the cybercrime legislation in Singapore is also named as Computer Misuse Act, the author uses ECMA and SCMA to refer to the Computer Misuse Act in England and in Singapore respectively.

as those of the US and the CoE. Originally, England tried to employ the then existing criminal provisions to regulate cybercrime, including the Criminal Damage Act 1971, the Theft Act 1968, and the Forgery and Counterfeiting Act 1981.[959] However, the attempts of applying these Acts to computer wrongdoings were proved to either expand their criminalisation scope or lead to irrational conclusions. For instance, before applying the Criminal Damage Act to cybercrime, the 'property' that being damaged must be expanded to include 'intangible' things; the Theft Act could in fact apply to all cyber offences because there would always be some abstraction of electricity in cybercrime; the application of the Forgery and Counterfeiting Act would suggest a computer was deceived which could not because a computer could not think. Consequently, the significance of new and specific legislation was recognised. The introduction of this new legislation was swift. In 1989 the first Private Member's bill concerning crimes involving computers was submitted to the Parliament,[960] with the ECMA being enacted one year later. In the light of experience accumulated in applying traditional criminal provisions to computer crimes, drafters of the ECMA 1990 chose to rely upon the flexibility of traditional criminal provisions to deal with most computer crime, mostly traditional crimes facilitated by computers, and to enact new provisions to tackle the crimes that traditional criminal provisions could not deal with, the genuine cybercrimes. Moreover, the ECMA 1990 protects the security of the data stored on a computer rather than computer the device, arguably to avoid the confusion between the intangible data and the tangible computer.[961]

Singaporean scholars and legislators had not much discussion about whether traditional criminal provisions could be applied to crimes involving computers.[962] One possible reason to this phenomenon is the fact that, the Singapore Computer Misuse Act (SCMA) was largely borrowed from its Legislative Source Key, the ECMA, the Canadian Criminal Code and the South Australia Evidence Act.[963] Since England, Canada, and Australia had already tried and failed in the application of traditional criminal provisions to crimes involving computers, there seems to be no point of Singapore to try again. Partly due to the lack of experience of

[959] For the details of the attempts see Chapter 5 Cybercrime Legislation in England.

[960] To be noted, this Private Member's bill was not passed. Later, another Private Member's bill was submitted, and ultimately became the England Computer Misuse Act 1990 after debate.

[961] For more details of the approach taken by the Computer Misuse Act 1990, England, see Chapter 5 Cybercrime Legislation in England.

[962] For more detailed information on the evolution of criminal provisions regarding cybercrime, see Chapter 6 Cybercrime Legislation in Singapore.

[963] Section 12A(2) of the Computer Misuse Act, Singapore.

applying criminal provisions to computer wrongdoings, the Singapore does not establish a consistent approach in the SCMA. On the one hand, learning from the ECMA 1990, the SCMA distinguishes between the genuine computer crime and traditional crimes facilitated by computers. On the other hand, the SCMA does not only focus on the security of data, as the ECMA 1990 does. Instead, it also focuses on the function of the computer, learned from another Legislative Source Key – the Canadian Criminal Code.[964]

Among all the selected jurisdictions and the CoE, the US was the forerunner in the field of criminalising cyber wrongdoing, with China being the last. Even when it came to the attempts to regulate cyber wrongdoing, China was around two decades late. This may be explained by the fact that it was not until 1994 that computers in China were able to connect to the Internet,[965] which was rather late compared with other selected jurisdictions. Thus, not only crimes involving computers, but also the discussion on such crimes, appeared much later in China.

Comparing the attempts made before the promulgation of specific legislation on cybercrime, the initial intention of the selected legal regimes was to apply traditional criminal provisions to crimes involving computers. However, these existing provisions were either not applicable or were inappropriate to apply.[966] This result echoes and proves what has been discussed in the Introduction Chapter: cybercrime challenges the criminal law, and there is a subsequent necessity for new and specific criminal provisions.

7.2.1.3 Key amendments to cybercrime legislations: an expanding process

In order not to infringe online freedom excessively, the selected jurisdictions intentionally limited the criminalisation scope of computer-specific legislation in the beginning, as mentioned in previous Chapters. However, netizens frequently complain of the infringed freedom in the online world. The amendments in the later period must have expanded the reach of cybercrime legislations in the selected legal regimes. The US has amended its CFAA eight times, Singapore four times, China and England the least, twice. What are these

[964] For more details on how Singapore learns from its legislative source keys, see Chapter 6 Cybercrime Legislation in Singapore.

[965] See CNNIC, '1994~1996 互联网大事纪' (Internet Events 1994~1996), 26 May 2009, available at http://www.cnnic.net.cn/hlwfzyj/hlwdsj/201206/t20120612_27415.htm. Last visited April 2016.

[966] For more details on how the legal regimes found the traditional criminal provisions inappropriate or inapplicable to cybercrime, see the attempts made by the selected jurisdictions and the Council of Europe in previous Chapters.

amendments, and to what extent these amendments expanded the scope of cybercrime legislation, are the two issues addressed in the following.

Chinese cybercrime legislation has been amended twice through Amendments (VII) and (IX) to the Criminal Law, in 2009 and 2015 respectively. After being revised in 1997, the Criminal Law indeed could deal with some of computer crimes. As the rise in the popularity of personal computers, they increasingly became the target of crimes. However, the security of personal computers, as well as the security of the data stored on the personal computers, was not covered by the CL 1997. Therefore, in 2009 the Amendment (VII) inserted two subsections to protect personal computers and the data stored on personal computers. However, these two new subsections did little to deter computer crime. Online fraud and hacking still happened widely and frequently, and more and more computer crimes were committed through the information network. Thus, to solve this problem and combat crimes using the information network, Amendment (IX) was enacted to strengthen the protection of information network in 2015. With this Amendment, the scope of computer crime was broadened to include the criminal liability of network service providers, and the assistance and preparation of crimes targeting or facilitated by computer technology. These expansions made to the Criminal Law have been viewed as a big step forward to enhance the security of computer and network.[967] However, a big step forward toward criminalisation often suggests a big step backwards in terms of enhancing online freedom.

The US has issued eight Amendments to its CFAA in the last three decades. These eight Amendments reflect a trend to extend the coverage of the CFAA.[968] The expansions on the term 'protected computer' can serve as an example of this trend. In the CFAA 1984, 'protected computers' were those 'affecting federal interests', and essentially referred to computers used for, or affecting those used for, financial institutions or the US government. Two years later, in the 1986 Amendment, a subpart was inserted with regard to the 'computers affecting federal interests'. That is, if 'two or more computers were involved in committing this offence, and not all of them were in the same state', the computers involved were regarded as affecting federal interests.[969] As a result of adding this subpart, the federal

[967] See e.g. 'Interpretation on Provisions Regarding Network in the Amendment (IX) to the Criminal Law by Legislative Affairs Commission of the Standing Committee of National People's Congress', 18 November 2015, available at http://www.npc.gov.cn/npc/fzgzwyh/2015-11/18/content_1952070.htm. Last visited February 2016. For more details see Chapter 2 Cybercrime Legislation in China.

[968] For the details of this trend see Chapter 4 Cybercrime Legislation in the US.

[969] 18 U.S.C. § 1030(e)(2) (1986).

legal agencies were given jurisdiction over activities conducted between different states within the US federation. Then, in the amendments made in 1988 and 1990, the scope of the term 'financial institution' used to determine 'computers affecting federal interests' was broadened to include not only the American banks but also the agencies or branches of foreign banks. Subsequently, in 1996, the wording 'computers affecting federal interests' was replaced by 'protected computers', which referred to 'all computers located **within** the territory of the US and connected to the Internet or an inter-state or foreign network'. This term was further expanded to include computers located **outside** US territory in 2001 and 2008, as long as that computer was used in a way that 'affects interstate or the foreign commerce or communications of the United States'. Consequently, unless a computer is not connected to the Internet or any other inter-state or foreign network, it is protected by the CFAA, wherever it locates. The expansions and the wordings used to describe the 'protected computers' clearly show the position of the US as trying to prosecute any crime involving computers that potentially threatening the security of the US. This phenomenon demonstrates the aim of the US to protect its governmental interests, including financial interests and national security, to the utmost extent.

For the case of England, two amendments were made to its ECMA, in 2006 and 2015 respectively. The England Police Justice Act (EPJA) 2006 was issued to meet the requirements of signing the CoC, as well as to respond to the demand of tightening the law regarding computer crime presented by different domestic groups.[970] The England Serious Crime Act (ESCA) 2015 was published in response to the proposal raised by the UK Government's Cyber Security Strategy on the unauthorised use of computers causing serious damage, and to meet the requirement to protect the information systems in the European Parliament and European Council Directive 2013/40/EU.[971]

The wordings of these two amendments show the changed position on criminalising cyber wrongdoings in England, from taking online freedom as the priority to protecting national interests. Admittedly, during the Parliamentary debate on the EPJA 2006, some members raised the threats to national security presented by cyber-terrorism to emphasise the importance of tightening the law with regard to computer crime. However, the main

[970] For details of the demand of tightening the ECMA, see Chapter 5 Cybercrime Legislation in England.

[971] See Chapter 5 Cybercrime Legislation in England. Sections 127 and 128 of the Explanatory Notes of England Serious Crime Act, available at http://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/2. Last visited September 2015.

considerations of legal scholars, non-governmental organisations, legislators and the Law Commission were in fact the effectiveness of the ECMA, its potential infringement of online freedom, and the potential abuse of governmental power. With these concerns, although England expanded the scope of the ECMA, such expansion was limited: only hacking in the pursuit of further crimes and supplying articles that could be used as hacking tools were introduced as new offences. While still, the EPJA 2006 shows some clues for changes. The wording of section 3 replaced by EPJA 2006 (i.e. unauthorised act 'in relation to computer') demonstrates that the focus of the ECMA was shifted from data to computer the device, from 'unauthorised modification of computer material' to 'unauthorised act in relation to a computer'. This new position is affirmed by the ESCA 2015. The focus of the newly introduced offence under the ESCA 2015 is no longer 'computer material' once used; instead, the 'unauthorised acts in relation to computer' became the *actus reas*. Accordingly, the prevented damage is not the one caused to the confidentiality, integrity and availability of computer material, but to the personal, societal and national security, such as the security of the water supply system or the health services. Moreover, neither the EPJA 2006 nor the ESCA 2015 explains the term 'unauthorised act in relation to computer'. Thus, what constitutes the term 'in relation to' is left untouched in the cybercrime legislation, which has a great possibility being interpreted in a broad way to cover future changes in cybercrime. All in all, it seems the English cybercrime legislation is beginning to shed a wider net on criminalisation so as to protect national interests, although it was once intended not to infringe online freedom.

The four Singaporean Amendments to the SCMA 1993 also imply a trend of expansion, both in the scope of criminalisation and in the power granted to the agencies to enforce the SCMA, especially the latter. The SCMA 1993 empowered the police to demand access to and check the operation of any computer that is reasonably suspected in the use of offence, and require the suspect to provide them with reasonable assistance.[972] This provision was replaced with a new one by the SCMAA 1998. Udner the new provision, police officers must obtain the consent from the Prosecution first if they, for instance, use the computer involved to search any data contained in or available to such computer.[973] However, no consent from the Prosecution was compulsory to have access to and inspect and check the operation of any

[972] Section 14 of the Computer Misuse Act, Singapore, 1993.

[973] Section 14 of the Computer Misuse Act, Singapore, 1998.

computer that is reasonably suspected of being used in any offence.[974] Subsequently, the SCMAA 2003 entitled the Minister to empower any person or organisation to take necessary measures to prevent or counter any threat to a computer system, which can affect the national security, essential services, defence or foreign relations of Singapore.[975] The SCMAA 2013 takes a step further and allows a person or organisation to disclose information they obtained under the Minister's certificate for cases with respect to national security, essential services or defence of Singapore or the foreign relations of Singapore.[976] The consideration behind these extensions, as emphasised by the members of Parliamentary debate, is to strengthen the protection of the economic and national security of Singapore.[977]

Generally speaking, it is difficult to compare which one of the four jurisdictions has expanded its cybercrime legislation the most. However, divergencies on different perspectives of expansions can be noticed. China mainly expands the ways of conducting cybercrime. By two Amendments, China not only has introduced offences that other jurisdictions criminalise, such as unauthorised access and misuse of devices, it has also introduced offences that other jurisdictions do not criminalise, such as failing of supervising the information network, setting up websites for distributing illegal information and assisting those intending to commit crimes through the information network. The US has mainly expanded the concept of 'computer'. As a result of such expansion, the US police have investigative power over computers that almost all around the world. The expansion in England mainly reflects in the legislative approaches of the cybercrime legislation. In the ECMA 1990, only behaviours damaging computer material shall be punished, while now impairing the operation of a computer shall also be punished. Singapore is remarkable for the expansions of the enforcement powers in the SCMA.

In sum, it can be observed that the legislations of the various selected jurisdictions on cybercrime are all expanding. Moreover, judging from the past experiences and the developing information technology, this expanding trend will continue.

---

[974] *Ibid.*

[975] Section 15A of the Computer Misuse Act, Singapore, 2003.

[976] Section 15A of the Computer Misuse Act, Singapore.

[977] See e.g. Assada Endeshaw, 'Computer Misuse Law in Singapore', *Information and Communication Technology*, vol. 8 1(1999): 5-33, p. 18.

7.2.2 National security as the main motivation behind the expanding process

The experiences of all the selected jurisdictions on amending cybercrime legislation indicate the expanding tendency. The factors given by the selected jurisdictions influencing this trend appear to be similar, which are to cover the gap between law and practice in the earlier stage, and to protect national security in more recent years. In the earlier stage of the legislative process, China, the US, England and Singapore all demonstrated some reluctance to implement stringent control over cyberspace, and struggled to find a way to regulate cyberspace without excessively infringing online freedom. Thus, in this period they did not draft or interpret criminal provisions broadly. Later, as information technology started to be manipulated to launch attacks against computers used in critical sectors such as essential emergency services and national defence, covering the gap between law and practice gave priority to deterring attacks threatening national security, only the extent to which the priority has been given differs among the selected jurisdictions.

China has not in fact emphasised the protection of national security in criminal law explicitly to justify its preference to expand the cybercrime legislation. The reason for the expansion in 2009, as implied by the inserted criminal provisions, was to cover the gap that had opened up by the developments in information technology and the increased popularity of personal computers. As for the amendments made in 2015, the aim of enhancing the security of the information network was cited as the main reason, according to the 'Explanation to the Amendment (IX) to the Criminal Law of the People's Republic of China (Draft)' (hereafter the Explanation).[978]

However, although the laws does not explicitly emphasise 'national security', the aim of enhancing 'national security' still serves as a motivation to tighten the law, and the online freedom is subsequently infringed. The space for lawful online activities is becoming increasingly restricted through Amendments, Judicial Interpretations, and administrative regulations. For instance, it seems the simple explanation for the Amendment (IX) as to protect the information network is not convincing, and enhancing the protection of national security is the key drive. Firstly, as analysed in the Chapter on China, 'information network'

[978] Available at http://www.npc.gov.cn/npc/lfzt/rlys/2014-11/03/content_1885123.htm. For its English translation see http://chinalawtranslate.com/%E5%85%B3%E4%BA%8E%E3%80%8A%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E5%88%91%E6%B3%95%E4%BF%AE%E6%AD%A3%E6%A1%88%EF%BC%88%E4%B9%9D%EF%BC%89%EF%BC%88%E8%8D%89%E6%A1%88%EF%BC%89/?lang=en. Last visit September 2015.

in fact belongs to 'computer', thus it seems less necessary of establishing new offences to protect the information network that had already been protected. Secondly, the gaps that Amendment (IX) intends to cover, the precise acts it intends to prohibit, the relationship between the newly inserted provisions and previously existing provisions, none of these issues is touched upon in the Amendment (IX), or in the Explanation. This phenomenon makes the reason that to protect the information network even weaker because without addressing these issues the position of the newly inserted offences in the criminalising system appears unclear. Especially, whether the newly inserted offences were to enhance the punishment of such behaviours, to emphasise the punishable nature of such behaviours, or others. Scholars and politicians have also noticed this phenomenon. As already mentioned in the Chapter on China, they point out when explaining the necessity of the Cyber Security Law that to prevent computers and the information network from being manipulated by terrorists is the main motivation of tightening the law.[979]

The US has expanded the scope of the CFAA to protect the economic and national security. From the very beginning, the US emphasised the threats posed by cybercrime to its economic and national security, and this is also the main reason given for the US expanding its law frequently and dramatically. In an effort to reverse this tide of expansion, the American scholars have rightly raised the right to privacy. However, the security of the US appears to take precedence, judging by the continuous expansion. It seems that the US intends to prevent any threat to any computer that may affect its inter-state or foreign commerce and communications, wherever this computer locates. Therefore, it can be expected that the US will further extend the scope of the CFAA in the future.

When establishing the first legislation on cybercrime, England and Singapore did not mention the protection of national security. However, as time went by, both England and Singapore noticed the threats to their national security presented by cybercrime. Thus, when amending the ECMA and the SCMA, both of them have referred to national security. For instance, section 3ZA, the one inserted by the Serious Crime Act 2015 of England, states especially that unauthorised acts in relation to a computer causing damage to the national security of any

[979] For more detailed information of how national security serve to justify the necessity of tightening the law, see Chapter 2 Cybercrime Legislation in China. See also, e.g. Article 1 of the Cybersecurity Law (Draft), available at http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm. Last visited February 2016. It should be noted that the Cyber Security Law is not regarding cybercrime. It is an administrative law mainly regulating behaviours of government, Internet service providers and information technology professionals.

country will get a heavier punishment than normal unauthorised acts. Singapore also emphasised the enhanced punishment for unauthorised hackings to the computer or data that 'is used directly in connection to the security, defence…of Singapore'.[980] Nonetheless, there are some differences between these two jurisdictions with respect to the extent to which the concern over national security influences the legislation. Claims were raised from the perspective of online freedom in both England and Singapore. This claim was sustained in the British parliament, and so the amendments made to the ECMA were relatively minor. As the Parliamentary debate shows, the newly introduced offence under section 3A of the ECMA was already covered by section 3, and English law merely intends to emphasise the punishable nature of such serious crime.[981] The fate of the argument concerning online freedom is different in Singapore. Among the four amendments, three of them were justified by the need to protect national security. Furthermore, the SCMAA 1998, possibly borrowing from the US, introduced the concept of the 'protected computer' to safeguard the security of Singapore.

Generally speaking, the long period of attempts and discussions about the criminalisation of cyber wrongdoings among the selected jurisdictions and the CoE reflects the difficulty on striking an adequate balance when addressing a new area of potential criminal activities. In the field of cybercrime legislation, this balance is how to regulate cybercrime while not excessively restricting online freedom. It becomes the main issue throughout the continued fight against cybercrime: set a wide net for criminalisation and thus restrict online freedom, or try not to intervene in online activity and thus accept a higher risk of cybercrime. Different priorities in different periods demonstrate the dynamics between online freedom and cybercrime criminalisation.

Judging from the expanding process and the motivations behind, the balance had been tipped towards online freedom in the early stage. Eventually, it began to tip towards cybercrime criminalisation so as to deter cybercrime, and further to safeguard national security. To be clearer, the fear about the information network and computers being manipulated to damage national security has gradually become the main concern of all the selected jurisdictions. Gradually, this fear drove the jurisdictions to remove the limitation on criminalisation and adopt more stringent regulations to govern the online world. The only difference is the degree

[980] Article 9 of the Computer Misuse Act, Singapore.

[981] 'Impact Assessment of Serious Crime Bill: Computer Misuse Act 1990 – Aggravated Offence', 2 June 2014, available at http://www.parliament.uk/documents/impact-assessments/IA14-21B.pdf. Last visit September 2015.

to which jurisdictions have expanded the scope of cybercrime legislation. For instance, the argument concerning online freedom was sustained in England while ignored in Singapore. The transition from online freedom to national security echoes with the transition from freedom to crime control observed in the real world. As David Garland depicts, freedom has given way to 'efforts at consolidation and the re-imposition of order and control'.[982]

7.2.3 The capacity of judges on adjudicating cybercrime cases

Uncertainties arise in legal provisions if the judges interpret the terms and wordings broad, and such situation often happens when there is limited legislative guidance. In the field of cybercrime, judges often encounter the lack of legislative guidance. How judges decide in such a situation and the extent to which they can interpret the law is very relevant to the development of cybercrime legislation. On this very issue, judges in the US and England and judges in China demonstrate different positions.

Before the promulgation of the specific provisions to tackle crimes involving computers, jurisdictions have tried the existing legal statutes, including applying traditional criminal provisions in cyberspace and applying cybercrime provisions to new forms of cyber wrongdoings. In doing so, judges become the front line of regulating the cyber wrongdoings in question. However, it is not long before judges realise that in this specific field, far-reaching reforms cannot be achieved only through judicial interpretation. Thus, judges become passive in extensively interpreting criminal provisions and prefer to wait for legislative guidance, including judges of the US and England, the two jurisdictions with common law tradition.

For the case of the US, diverging lines of interpreting provisions on the same issue weakens the capacity of judges. In the case *International Airport Centers, LLC v. Citrin*[983] the Seventh

[982] David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society*, USA: The University of Chicago Press, 2001, pp. 197-198.

[983] *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). The defendant, Citrin, was an employee of the plaintiffs 'IAC'. IAC lent Citrin a laptop to use to record data that he collected in the course of his work in identifying potential acquisition targets. Citrin decided to quit IAC and go into business for himself, in breach of his employment contract. Before returning the laptop to IAC, he deleted all the data on it - not only the data that he had collected but also data that would have revealed to IAC improper conduct in which he had engaged before he decided to quit. Ordinarily, pressing the 'delete' key on a computer (or using a mouse click to delete) does not affect the data sought to be deleted; it merely removes the index entry and pointers to the data file so that the file appears no longer to be there, and the space allocated to that file is made available for future write commands. Such 'deleted' files are easily recoverable. But Citrin loaded into the laptop a secure-erasure program, designed, by writing over the deleted files, to prevent their recovery. IAC had no copies of the files that Citrin erased. The Seventh Circuit held that Citrin had violated the 18 U.S.C. § 1030(a)(5)(A) and (a)(5)(B).

Circuit Court of Appeal held the defendant had violated the CFAA because he erased the data stored on a laptop belonging to his firm after his employment contract was ended and before his authorisation to the laptop was rescinded. The court concluded that the defendant had broken his duty of loyalty terminated his agency relationship – the only basis for his authority to 'return or destroy' data on the laptop, and therefore his behaviour constitutes 'without authorisation'.[984] In contrast to this case, the Ninth Circuit Court reached an opposite conclusion when considering whether an employee had acted 'without authorisation'. Namely, in the similar case *United States v. Nosal*[985] the court found the defendant non-guilty by maintaining that Nosal could not act without authorisation before his former employer rescinded his authorisation. Both defendants had some authority to use the computer, while they received opposite judgements. In fact, judges themselves had also noticed and admitted this divergence, such as the US Court of Appeals for the Ninth Circuit.[986]

Situations the English judges face are almost the same, and they also sometimes cannot reach a consensus on the same issue. In the case *R v. Gold and Another*[987] the defendants were convicted in the first instance. Later, the Court of Appeal ruled the defendants did not violate the law because the electronic impulses generated by the defendants could not constitute

---

[984] *Ibid*.

[985] *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012). From April 1996 to October 2004, Nosal worked as an executive for Korn/Ferry International (Korn/Ferry), an executive search firm. When Nosal left Korn/Ferry in October 2004, he signed a Separation and General Release Agreement and an Independent Contractor Agreement. Pursuant to these contracts, Nosal agreed to serve as an independent contractor for Korn/Ferry and not to compete with Korn/Ferry for one year. In return, Korn/Ferry agreed to pay Nosal two lump-sum payments in addition to twelve monthly payments of $25,000. Shortly after leaving his employment, Nosal engaged three Korn/Ferry employees to help him start a competing business. The indictment alleges that these employees obtained trade secrets and other proprietary information by using their user accounts to access the Korn/Ferry computer system. Specifically, the employees transferred to Nosal source lists, names, and contact information from the 'Searcher' database — a 'highly confidential and proprietary database of executives and companies' — which was considered by Korn/Ferry 'to be one of the most comprehensive databases of executive candidates in the world'. Nosal was charged under 18 U.S.C. § 1030(a)(4), under which 'knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorised access, and by means of such conduct furthers the intended fraud and obtains anything of value' is criminalised.

[986] The US Court of Appeals for the Ninth Circuit admitted in the judgement of *United States v. Nosal* that

'Some courts… generally held that authorised access to a company computer terminated once an employee acted with adverse or nefarious interests and against the duty of loyalty imposed on an employee in an agency relationship with his or her employer or former employer.

Other courts … reasoned that the CFAA is intended to punish computer hackers, electronic trespassers and other "outsiders" but not employees who abuse computer access privileges to misuse information derived from their employment.'

For detailed information on the divergence among judgements on similar cases in the US, see Chapter 4 Cybercrime Legislation in the US.

[987] *R v. Gold and Another,* [1988] 2 WLR 984, [1988] AC 1063, [1988] 2 All ER 186. The defendants had hacked a remote computer system, by the unauthorised use of the passwords and IDs of other users of the system. For more details see http://swarb.co.uk/regina-v-gold-and-schifreen-hl-21-apr-1988/. Last visited January 2016.

'false instrument' under the purpose of the law. The two defendants were thus acquitted. In the House of Lords Proceedings, the Lords upheld the decision of the Court of Appeal.

These cases and contradictory judgements can prove the insufficient capacity of American and English judges when adjudicating cybercrime cases without proper legislative guidance. As Colin Tapper once suggested, the function of the judiciary is 'to decide disputes about past facts by the application of current rules; it is not to provide for possible future disputes about other facts by pronouncing new rules.'[988] Thus, even though the judiciary has the authority to create new criminal laws, it should be reluctant to do so, as the UK House of Lords once suggested.[989] Therefore, it is better for the judiciary to wait for the legislative response when they encounter problems in dealing with computer crimes. By doing so, they will not make far-reaching interpretations.

People may assume that in China - a non-common law system, judges would be more relunctant of making broad interpretations compared with judges in common law systems. Indeed, similar to the judges in the US and England, individual judges in China play a rather passive role in law-making. However, the Supreme People's Court (SPC) of China, as the highest judicial organ, has a significant function in de facto law-making by issuing Judicial Interpretation. As mentioned in the Chapter on China, the SPC can issue Judicial Interpretations to guide individual judges on how to apply legal provisions and the extent to which these provisions can be extended, including the situations where certain legal provisions can apply, and these Judicial Interpretations must be followed in judicial practice.[990] By doing so, the judges in the SPC as a whole can influence the application of the criminal law in judicial practice, and therefore make far-reaching interpretations. In the cybercrime field where legislation frequently fell behind the practice, the guidance provided by the SPC can, under many circumstances, brige the gap between law and practice and be more significant than the legislation.

---

[988] Colin Tapper, 'Judicial Attitudes, Aptitudes and Abilities in the Field of High Technology', *Monash University Law Review*, vol. 15 (1989): 219-228, p. 220.

[989] *Myers v. Director of Public Prosecutions*, [1965] A.C. 1001, 1022. See also Douglas H. Hancock, 'To What Extent Should Computer Related Crime be the Subject of Specific Legislative Attention?' *Albany Law Journal of Science and Technology*, vol. 12 (2001): 97-124, p. 97. For more detailed information on this issue see Chapter 5 Cybercrime Legislation in England.

[990] For the details of the Judicial Interpretation in Chinese context, see Chapter 2 Cybercrime Legislation in China.

7.2.4 Unsolved issue of defining cybercrime

'Cybercrime' has always been a hot topic not only for the academic but also for the public. Nonetheless, cybercrime is seldom clearly described or defined. Despite many scholars and legislators have proposed dozens of definitions on 'cybercrime', till now none of the definitions has become widely accepted. This phenomenon raises three questions: (1) what are the reasons for the absence of a widely accepted definition, (2) is it possible to define cybercrime that can be widely accepted, and (3) is a definition complusary for adequate legislation?

There is no authoritative or generally accepted definition of cybercrime (or computer crime) in China. As early as in 1983, Yang Yuguan, a legal scholar, regarded computer crime as a unique kind of crime, and rightly pointed out that a computer could be both the target of crime, and the tool of crime. According to him, 'computer crime' is 'the activity that destroys or steals a computer or any part of the computer, or activity that uses a computer to commit theft or corruption'.[991] According to Yang, computer crime included three types of crime: the destruction of a computer or any part of a computer, the theft of a computer or any part of a computer, and the use of a computer to commit theft or facilitate corruption.[992] This definition and categorisation laid the foundations for the definitions and research following, although too broad in terms of today's understanding of cybercrime as it includes stealing a computer. In 1990, Chen Lihua also regarded computer crime as a unique category of crime. Moreover, he distinguished between the activities damaging computers from those damaging property. Under his definition, 'computer crime' is 'activities which, using a computer as a tool, damage public or private property and damage the computer device or system'.[993] By mentioning the crime of damaging computers, he was referring to activities that damage the software of a computer, as well as causing damage to the hardware of a computer through violence.[994] The following definitions proposed in the early 1990s echoed these two definitions to a greater or lesser degree, and the difference among definitions was whether computer crime was a unique category of crime or could be distributed across various

[991] Yang Yuguan, '计算机与犯罪' (Computer and Crime), *Zhengfa Luntan* (Tribune of Political Science and Law), 2(1986): 78-80, 55, p. 78.

[992] *Ibid.*

[993] Chen Lihua, '计算机犯罪及立法探讨' (Discussion on Computer Crime and Its Legislation), *Faxue* (Law Science), 1(1990): 42-44, p. 42.

[994] *Ibid*.

categories. Until the middle of the1990s, just before the promulgation of the Criminal Law 1997, a group of scholars realised that the definitions presented by Yang and Chen were so broad that destroying a computer screen by an act of violence would fall under their definitions.[995] Thus, in 1996, Yang Weiguo defined computer crime in a way that distinguishing it from traditional crimes. According to him, 'computer crime' is those, using computer technology as their instrument, committed by illegally operating a computer and/or destroying the computer's information system.[996] This definition clearly covers the crimes that damage a computer, but not the crimes that damage property. In later years this definition gained much support among leading scholars in the field of computer crime.[997] Although not recognised explicitly, Yang Weiguo's definition gradually became widely accepted, judging from the fact that there has been little discussion about the definition of computer crime after it. Instead, more and more attention has been given to new forms of computer crime, such as a Distributed Denial of Service (DDoS) attack, and the issue of jurisdiction.

One may expect that the Convention on Cybercrime, as an international legal instrument, can provide a definition on cybercrime. However, it does not define cybercrime either. Fearing that a definition of cybercrime may lead to difficulties in the process of attracting signatories and raise more issues than it could solve, and also in order to avoid infringement of domestic legal regimes and cultures, the drafters of the CoC decided to leave the definition of cybercrime to the individual States.[998] They maintained that a Convention with more signatories would be more helpful than a one with clear guiding definitions of cybercrime and its elements.[999] However, some hold a different opinion, as they argued that the CoC would be more valuable if it provided a definition of cybercrime or its elements and thus set a standard for criminalisation.[1000]

---

[995] See e.g. Jiang Ping, '计算机犯罪初探' (Exploring Computer Crime), *Policing Studies*, 4(1995): 33-36.

[996] Yang Weiguo, '计算机犯罪立法有关问题初探' (Computer Crimes and Its Relevant Legal Issues), in *The Proceedings of the 11th National Computer Security Conference*, Beijing: China Academic Journal Electronic Publishing House, 1996, pp. 30-34.

[997] See e.g. Zhao Bingzhi and Yu Zhigang, '论计算机犯罪的定义' (The Definition of Computer Crime), *Xiandai Faxue* (Modern Law Science), 5(1998): 7-10.

[998] See e.g. Shannon L. Hopkins, 'Cybercrime Convention: A Positive Beginning to a Long Road Ahead', *Journal of High Technology Law*, vol. II 1(2003): 101-122, pp. 113-115. See also The Council of Europe, Recommendation No. R (89) 9, p. 13.

[999] See e.g. Jonathan Clough, 'The Council of Europe Convention on Cybercrime: Defining "Crime" in a Digital World', *Criminal Law Forum*, vol. 23 (2012): 363-391.

[1000] *Ibid*.

The US legislators choose not to define computer crime in the CFAA as well, and therefore, the term 'computer crime' implies different connotations for different scholars. As early as in the 1970s, Donn Parker regarded 'computer abuse' as traditional crimes that committed using computer technology. Specifically, he defined 'computer abuse'[1001] as 'any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made a gain'.[1002] Two key elements can be identified from this definition: the use of computer technology, and making a gain. This definition is in fact quite similar to the one proposed by the Chinese scholar Chen. To both of them, the use of a computer is the essential differentiator from other crimes. Unlike in China, this definition was criticised in the US context. Firstly, the connection between *computing* and *abuses* is broad.[1003] For instance, the question that to what extent using a computer constitutes 'an incident associated with computer technology' is not clear under this definition. Secondly, the meaning of 'making a gain' is not clear as regards whether it only refers to monetary gain or to all kinds of gain. If it only refers to monetary gain, then hacking for State secret, for instance, would not be included. If it refers to all kinds of gain, this requirement becomes useless to qualify computer crime, since any crime can potentially result in a given form of gain. Consequently, in the manual Parker prepared for the Department of Justice in 1989, he deleted 'loss' and 'gain' – the terms that raise different concerns, and redefined computer crime as 'any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation, or prosecution'.[1004] However, this new definition had become extremely broad because of the deletion. Without adequate requirements, it seems Parker interpreted 'computer abuse' as any form of abuse as long as it had an 'essential' connection with computer technology. In fact, this is exactly what he means. In the book published in 1998, he firstly replaced the term 'computer abuse' with the term 'cybercrime' and secondly he defined 'cybercrime' in a way, according to himself,

[1001] Because back then scholars were discussing whether 'computer crime' was an appropriate term to describe all computer wrongdoings. To avoid misunderstanding, Donn Parker adopted the term 'computer abuse'.

[1002] Donn B. Parker, *Crime by Computer*, New York: Charles Scribner's Sons, 1976, p. 12.

[1003] Rob Kling, 'Computer Abuse and Computer Crime as Organizational Activities', *Computer Law Journal*, 2(1980): 403-427, pp. 407-408.

[1004] National Institute of Justice, U.S. Department of Justice, prepared by Donn B. Parker, *Computer Crime: Criminal Justice Resource Manual*, August 1989.

'[encompassing] any abuse or misuse of information that entails using a knowledge of information systems.'[1005]

In this explanation Parker abandoned the term computer technology and used the word 'information'. This is because, as Parker clarified, 'loss of information' also encompassed stealing and misrepresenting information that was wider than the loss caused by manipulating computer technology.[1006] Thus, it is clear that the change from 'computer technology' to 'information' was to follow the developments in this field.[1007] It is also clear that referring to 'cybercrime' as being done *to* information or done *with* information is merely an updating of computer crime that 'has an essential connection with computer technology'.

Such a broad definition cannot escape criticism. Parker's definitions reflect the understanding of computer crime in its infancy to some extent: they encompass those crimes that computer technology (or information system in the later version) was involved in some way. As time goes by, the understanding of what cybercrime is has changed. Susan W. Brenner explicitly and rightly pointed out in 2001 that cybercrime was not merely traditional crime copied in cyberspace. Rather, it has its own characteristics.[1008] At the same period, Neal Kumar Katyal, a then Associate Professor, defined cybercrime as 'the use of a computer to facilitate or carry out a criminal offence'. He further explained that by saying 'facilitate or carry out a criminal offence', he referred to situations where a computer was the subject of a computer attack such as unauthorised access, or was a tool to carry out traditional crimes.[1009] Subsequently, instead of defining cybercrime, Susan W. Brenner divided cybercrime into three types: crimes with a computer as the target, with a computer as the instrument, and in which a computer is

---

[1005] According to Parker,

'Cybercrime encompasses abuse (harm done *to* information, such as causing the loss of usefulness, integrity, and authenticity) and misuse (harm done *with* information, such as causing the loss of availability, possession, and confidentiality). Beyond the direct loss of information, however, abuse and misuse may result in losses of, or injury to, property, services, and people…In my definition, cybercrime encompasses any abuse or misuse of information that entails using a knowledge of information systems.'

Donn B. Parker, 'Chapter 3: The Rise of Cybercrime', in Donn Parker, *Fighting Computer Crime: A New Framework for Protecting Information*, New Jersey: John Wiley and Sons, 1998.

[1006] *Ibid.*

[1007] *Ibid*.

[1008] Susan Brenner, 'Is There Such a Thing as "Virtual Crime"', *California Criminal Law Review*, vol. 4 6(2001): Article 1.

[1009] Neal Kumar Katyal, 'Criminal Law in Cyberspace', *University of Pennsylvania Law Review*, vol. 149 (2001): 1003-1114.

incidental.[1010] This classification was widely adopted, including the US Department of Justice in its Report.[1011] Scholars in the US gradually acknowledged that defining computer crime or cybercrime was a task that might never be accomplished, and identifying the roles performed by computers, as Professor Brenner had done, appeared much easier and meaningful. Thus, scholars started to use categorisation rather than definition in later research, and more or less relied on the categorisation Brenner presented.[1012]

In England, fearing that a definition would be either too narrow or too broad, the legislators provide no authoritative definition of 'computer crime' or 'cybercrime'. Thus, as in the US and China, legal scholars and institutions had devoted themselves to finding a proper definition. However, as the Law Commission stated in its report, academics and institutions had found it impossible to define 'computer crime' without being vague or too broad.[1013] Consequently, scholars left the definition of 'computer crime' or 'cybercrime' untouched in most research. Instead, research into the categorisation of computer crime has been regarded as more realistic. In this context, the efforts on determining computer crime in England primarily focus on the categorisation, according to the roles played by computers in the perpetration of a crime. The ways of categorising cybercrome include the followings.

In 1998, computer crime was devided into 'computer related crime' and 'computer assisted crime' by defining computer crime as 'any criminal act which involves one or more computers either as the object of the crime or as accessories in its commission'.[1014] The former refers to 'the computer or its contents as the subject of the criminal act', such as hacking, and the latter refers to 'the computer as merely an accessory in the commission of a crime which could at least in principle have been committed by other means', namely, those traditional crimes facilitated by computers.[1015] Five years later, Paul Barton and Viv Nissanka expressed their support of this two groups' categorisation of cybercrime. Avoiding

[1010] Susan Brenner, 'US Cybercrime Law: Defining Offences', *Information Systems Frontiers*, vol. 6 2(2004): 115-132.

[1011] Computer Crime and Intellectual Property Section, US Department of Justice, *The National Information Infrastructure Protection Act of 1996*, Legislative Analysis, 1996.

[1012] See e.g. Richard W. Downing, 'Shoring up the Weakest Link: What Lawmakers around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime', *Columbia Journal of Transnational Law*, vol. 43 (2005): 705-762.

[1013] For the discussion on this issue see Chapter 5 Cybercrime Legislation in England.

[1014] Richard E. Overill, 'Trend of Computer Crime', *Journal of Financial Crime*, vol. 6 2(1998): 157-162, p. 157.

[1015] *Ibid*.

defining computer crime directly, they interpreted computer crime as 'a multitude of offences ranging from virus dissemination, hacking and organised crime to terrorist rings that use a computer and computer networks in the commission of the offence'.[1016] At the same period, David Wall divided computer crime into three categories, including

> '(1) traditional crimes in which a computer has been used, in other words, the computer has provided information in some way, such as by searching the Internet to find potential victims;
>
> (2) traditional crimes for which network technology has created new opportunities, such as computer related fraud; and
>
> (3) the crimes which are solely the product of opportunities created by the Internet and which can only be perpetrated within cyberspace, such as hacking'.[1017]

Offences under the third group in Wall's categorisation were not widely accepted as computer crime. Later, in a report on cybercrime prepared by the UK Home Office, although cybercrime remained, once again, undefined,[1018] it was divided into two groups. These two groups are the 'new offences committed using new technology, such as offences against computer system and data, dealt with in the England Computer Misuse Act 1990', and the 'old offences committed using new technology, where networked computers and other devices are used to facilitate the commission of an offence'.[1019] These two groups echo the first two groups of Wall's categorisation, and group (3) of Wall's categorisation is not included. The categorisation under the Home Office report is widely adopted when analysing cybercrime in England. For instance, Jonathan Clough explained 'cybercrime' as 'one of a number of terms used to describe the use of digital technologies in the commission or facilitation of crime'.[1020] Mike McGuire subdivides cybercrime into cyber-dependent crimes and cyber-enabled crimes. The former refers to 'offences that can only be committed by using a computer, computer network, or other form of information and communication technology',

---

[1016] Paul Barton and Viv Nissanka, 'Cyber-crime - Criminal Offence or Civil Wrong? ', *Computer Law and Security Report*, vol. 19 5(2003): 401-405.

[1017] David Wall, 'What are Cybercrimes?' *Criminal Justice Matters*, 1(2004): 20-21.

[1018] Home Office, 'Cyber Crime Strategy', Presented to Parliament, March 2010, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf. Last visited August 2015.

[1019] *Ibid*.

[1020] Jonathan Clough, 'Data Theft? Cybercrime and the Increasing Criminalization of Access to Data', *Criminal Law Forum*, vol. 22 (2011): 145-170, p. 150.

such as hacking. The latter refers to 'traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other information and communication technology', such as computer related fraud.[1021]

Similar to the counterparts in China, the CoE, US and England, there is no definition of 'computer crime', or 'computer misuse', in the SCMA. In addition, since the SCMA is to a large extent borrowed from the ECMA, the debate on defining computer crime in Singapore is mostly based on the discussion on the same issue in England.[1022] The literature about cybercrime either leaves the definition untouched or cites the argumentations of British scholars. Considering the fact that British scholars did not succeed to present a generally accepted definition, Singaporean scholars have also left 'computer crime' undefined.

Comparing the attempts of defining 'cybercrime' in the selected jurisdictions and the CoE, scholars realised that a precise definition may raise more issues than it could solve after years of discussion. Therefore, they began to categorise cybercrime for a better understanding. Specifically, in order to decide the extent to which a computer is involved makes a crime a cybercrime, scholars categorised cybercrime on the basis of the roles performed by computers. The classification in England actually echoes the way of categorisation adopted in China, and the first two categories of the categorisation adopted by the US Department of Justice. This categorisation divides computer crime into two types: the computer participates as the target or as the tool.

In sum, it seems that although scholars have bent themselves towards the finding of a proper and generally accepted definition on cybercrime, this is actually a goal that may never be achieved. However, it is unrealistic to postpone the legislations against cybercrime until a generally accepted definition has been developed, and people have to possess basic knowledge of cybercrime to legislate against it. In this context, scholars have to consider alternative measures to determine the scope of cybercrime legislation. To some scholars, 'alternative measures' means the categorisation of cybercrime. Through years' of research, one categorisation is relatively widely accepted, in which computer plays as a target, as a tool, or merely an incidental element, although a global consensus is not reached on the issue to

[1021] Mike McGuire, 'Cyber Crime: A Review of the Evidence', *Home Office Research Report 75*, October 2013, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf. Last visited August 2015.

[1022] Assafa Endeshaw, 'Computer Misuse Law in Singapore', *Information and Communications Technology Law*, 1(1999): 5-33, p. 8.

which of the three groups cybercrime refers. Moreover, facts have shown that cybercrime legislations have been developing although without a generally accepted definition. Therefore, it seems that such a definition may not be necessary for legislation, as long as alternative measures can help to determine cybercrime.

7.2.5 Elements steering the scope of cybercrime

One reason for the absence of a generally accepted definition of cybercrime is its transitional nature and the evolving scope. Subsequently, jurisdictions hold different opinions regarding the definition and the scope of cybercrime, specifically, the extent to which computer is involved makes a crime a cybercrime. According to the above comparison, jurisdictions have reached at least one consensus: crimes in which computers plays as the target, the so-called genuine cybercrime, are cybercrime. The genuine cybercrime can generally be regarded as including illegal access, illegal interception, data interference, system interference and misuse of devices, with divergences among jurisdictions and the CoE. The analysis and comparison on the issues presented by the transitional nature and evolving scope of cybercrime are limited to the genuine cybercrime. In other words, this part only addresses the genuine cybercrime but not the traditional crimes facilitated by computers.

From the previous Chapters, three elements can be identified as setting up the scope of the genuine cybercrime. Different positions on interpreting these three elements reflect the divergences among the legislative approaches of the selected legal regimes. These three elements are:

(1) computer,

(2) unauthorised access, and

(3) fault element (i.e. *mens rea*).

7.2.5.1 The concept of computer

In the field of computer crime, the meaning of 'computer' remains undeniably central. However, although computer is a common word in daily usage, the rapid development of technology has constantly challenged the understanding of it.[1023] On the one hand, the device to which computer is referring keeps evolving. More and more household appliances are equipped with data storage and processing function to some degree. A washing machine can

[1023] Jonathan Clough, *The Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010, p. 52.

perform different programmes and modes, mobile phones can be used to receive and send e-mails, and global positioning system devices (hereafter after GPS devices) can guide people to their destination. On the other hand, data becomes increasingly targeted as being added, deleted and compressed. Data is stored on a computer. As the simplest response to the crimes targeting data, they can be treated as those targeting the computer. The rationale behind this treatment is that as soon as data is damaged, the computer on which data is stored is subsequently and inevitably damaged. Under this rationale, data is regarded as the computer. However, through analysing the concepts of 'computer' under the selected legal regimes, it can be learned that data is not, and cannot be, computer. Starting with an overview of the conception of 'computer' in the selected legal regimes, this section intends to address the issue 'what is computer'.

Since the scope of the term 'computer' directly affects the scope of 'computer crime', the selected jurisdictions and the CoE have all struggled to define it properly. Generally, three responses can be observed: China and the CoE adopt an alternative term - 'computer information system' and 'computer system' respectively. England leaves it to judges to decide. US and Singapore attempt a comprehensive and all-inclusive definition. In addition, cybercrime legislations in the CoE, England and Singapore explicitly treat 'data' differently from 'computer'.

Table 7.2 The subject of cybercrime legislations in the selected legal regimes

Jurisdiction	Subject	Example
China	computer information system	Whoever provides special programs or tools specially used for intruding into or illegally controlling **computer information systems** …
CoE	computer system, data	Computer system: … when committed intentionally, the access to the whole or any part of a **computer system** without right. Data: … when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer **data** without right.
US	computer	…intentionally accesses a **computer** without authorisation or exceeds authorised access…
England	data, computer	Data: …he causes a computer to perform any function with intent to secure access to any **program or data** held in any computer or to enable any such access to be secured. Computer: This subsection applies if the person intends by doing the act… to impair the operation of any **computer**.
Singapore	data, computer service	Data: For the purposes of this Act, a person secures access to any **program or data** held in a computer… Computer service: …secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any **computer service**…

In China, the legislation on computer crime is in fact based on the concept of 'computer information system'.[1024] The term suggests that criminal law prohibits activities that target a computer information system. The 'computer information system' refers to 'a system with an automatic data processing function, including computers, networking equipment, communications equipment, and automatic control equipment'.[1025] No material is available to explain why the Chinese legislature abandoned the term 'computer' in favour of the term 'computer information system'. Two possible reasons can be provided. As the first consideration, Chinese legislators prefer to define the basic term broadly to deal with any future development rather than limit themselves to a physical machine. As the second

[1024] See e.g. Article 258 of the Criminal Law, China.

[1025] Article 11 of the Interpretations of Several Issues on the Application of Law in Handling Criminal Cases about Endangering the Security of Computer Information Systems 2011, China, *Fa Shi* [2011] No. 19.

consideration, the legislators wish to emphasise that the computer is protected for its system, and further for the services it can provide.

The Convention on Cybercrime does not pinpoint the term 'computer' either. Rather, it adopts the term 'computer system' to describe one of the subjects it protects.[1026] Under the Convention, 'computer system' is defined as 'any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data'.[1027] It is clear that this definition focuses on the programmable function of the system, especially its data processing capability.

In the US, the legislature attaches an all-inclusive, while broad, definition of 'computer' to avoid ambiguity in criminal provisions and to make it applicable to future developments in information technological devices. Namely, 'computer' refers to all high-speed data processing devices performing certain work. It is defined as

> 'an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device'.[1028]

This definition focuses on the data processing functions of the computer, and includes data storage facilities and communications facilities directly connected to a device with a data processing function. Thus, in the US context, if a device, or a series of devices, has a data processing function, or is directly connected to such a device capable of storing or communicating data, it is the computer.

In England, the ECMA does not define 'computer'. Legal scholars and the Law Commission have considered and discussed two ways of defining 'computer'. One is providing an all-inclusive definition while at the same time listing certain devices that cannot be regarded as a computer, as the US does. The other one is leaving the term 'computer' undefined, and providing some guidance for judges to enable them to decide on a case-by-case basis when

[1026] See e.g. Article 2 of the Convention on Cybercrime, the Council of Europe.

[1027] Article 1(a) of the Convention on Cybercrime, the Council of Europe.

[1028] 18 U.S.C. § 1030(e)(1).

they deal with relevant situations.[1029] Since many legal scholars, the Law Commission, and the All-Party Parliamentary Internet Group (APIG) maintained that the absence of a definition has not led to more problems than the presence of one, and that judges had done a good job when interpreting the term 'computer', they proposed the second way – leaving 'computer' undefined.[1030] The legislators adopted this suggestion when drafting the ECMA, and have kept this approach in the amendments following.

Regarded as learning from the US by legal scholars, Singapore chose to define the term 'computer', and defined it in a sufficiently broad manner to encompass future changes. The term 'computer' is defined as:

> 'an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include:
>
> (*a*) an automated typewriter or typesetter
>
> (*b*) a portable hand-held calculator
>
> (*c*) a similar device which is non-programmable or which does not contain any data storage facility
>
> or
>
> (*d*) such other device as the Minister may, by notification in the *Gazette*, prescribe'.[1031]

It can be observed that this definition is almost a direct copy of the US definition, and the only difference is that the Singaporean one grants the Minister the power to exclude devices that should not be regarded as a computer.

[1029] For the detailed discussion on this issue, see Chapter 5 Cybercrime Legislation in England.

[1030] See the Law Commission, *Computer Misuse working Paper No. 110*, [6.23]. See also the Law Commission, *Criminal Law-Computer Misuse No. 186(1989),* [3.39].

[1031] Section 2(1) of the Computer Misuse Act, Singapore.

Comparison among the selected legal regimes shows that apart from England, the selected legal regimes provide a definition of 'computer', or 'computer information system' in the Chinese context and 'computer system' in the CoC context. It can be observed from the definitions of computer that they, in fact, refer to the function of processing data. However, with regard to the meaning of **processing data**, jurisdictions and the CoE hold different opinions.

Chinese legislation does not provide any detailed information or explanation of this. Computers in the ordinary meaning of the term, network equipment, communication equipment and automatic control equipment are explicitly included,[1032] whereas GPS devices and the chips in credit cards are not mentioned. According to the definition, since GPS devices can, following the program, process data, it belongs to computer; while the chips in credit card do not because they only contain data.

With regard to the definition under the CoC, the 'processing of data' means 'data in the computer system which is operated by executing a computer program', explained in the Explanatory Report of the Convention on Cybercrime (ERCoC).[1033] According to this explanation, a 'computer system' must possess the capability of automatically running a program. Therefore, GPS devices count as computer systems, because if the user types in a location, such a device can, by following the program, process the location and provide instruction as to how to get there. The peripherals to computer systems, like U-disk, do not fall within this definition. Neither does a printer or a screen.

The US and Singaporean definitions of computer also emphasise the function of processing data, including logical, arithmetic or storage functions. From the wording, the scope of 'computer' in the US or Singaporean context is broader than that of Chinese criminal law or the CoC, because storage devices and communications devices directly connected to a 'computer' in the ordinary meaning of the word are included. Specifically, according to the US and Singaporean definitions, peripherals such as U-disks and printers, are, in fact, a computer, or at least a part of a computer. Exclusions such as typewriters and handheld calculators are devices that can perform on their own, and they do not connect to any part of a computer in order to function. In this sense, GPS devices belong to a computer, while the

[1032] Article 11 of the Interpretations of Several Issues on the Application of Law in Handling Criminal Cases about Endangering the Security of Computer Information Systems 2011, *Fa Shi* [2011] No. 19.
[1033] Article 23 of the Explanatory Report of Convention on Cybercrime.

microchips in credit cards arguably do not fall into this category. This is because GPS devices can store and process data by themselves, and microchips in credit cards are not directly related to a computer, although they can store data. English law, as discussed in the Chapter on England, focuses more on the data stored on a computer rather than the computer itself. In this way, discussion on the scope of the term 'computer' appears less prevalent in England.

An important observation can be drawn from the preceding comparison and analysis that computer**,** which in its essence can process data**,** is distinguished from data. Thus, as data increasingly becomes the target of the genuine cybercrime, the term 'computer' is no longer a proper term used to refer to all the subject of cybercrime. According to the classification of cybercrime, in the genuine cybercrime computer serves as the target. Reading this together with the definitions of computer, one can notice that it is the function of the computer that being targeted. In other words, the computer is not targeted because it contains data. Rather, it is targeted because of its capability of processing data. However, some cybercrimes intend to destroy the function of computers, while more and more cybercrimes obtain or damage data. Although data is stored on computers, crimes targeting data and targeting the function of computers are different. Data to a computer is like wine to a bottle, and offenders can steal wine by pouring it into a glass without damaging the bottle. Similarly, offenders can obtain data by copying it into a U-disk without causing the computer unable to function. To put it in another way, the damage to data does not necessarily lead to damage to computer and *vice versa*. Thus, using the term computer to describe all sufferers of cybercrime is no longer appropriate. Moreover, as long as the legislators still regard the computer, or the function of computer, as the only target of the genuine cybercrime, the term 'computer' cannot be adequately defined, since the definition of computer needs to include data, which it does not and cannot include. To solve this problem, 'computer' and 'data' should be defined and treated differently in law.

7.2.5.2 Unauthorised access, exceeds authorised access, or access violating States' regulations

As a shared understanding of the genuine cybercrime, hacking is committed when the access is unauthorised. However, not all the selected legal regimes refer to 'unauthorised access' when determining whether a crime is a cybercrime. Instead, they have corresponding wordings, such as 'in violation of State's regulation'. Moreover, by adopting different corresponding wordings, the selected legal regimes endow different implications to them, and

encounter different issues in judicial practice. The corresponding wordings adopted in the selected legal regimes are shown in the Table below.

Table 7.3 Corresponding wordings regarding the term 'unauthorised access' in cybercrime legislations in the selected legal regimes

Jurisdiction	**Wordings**	**Example**
China	in violation of states' regulation	Whoever **violates States' regulations** and deletes, alters, adds, and interferes in computer information systems, causing abnormal operations of the systems and grave consequences…
CoE	access without right	… when committed intentionally, the **access** to the whole or any part of a computer system **without right**.
US	access without authorisation or exceeding authorised access	Whoever having knowingly **accessed** a computer **without authorisation or exceeding authorised access**…
England	cause (a computer) to perform any function unauthorised	he **causes a computer to perform any function** with intent to secure access to any program or data held in any computer… the access he intends to secure or to enable to be secured is **unauthorised**
Singapore	cause (a computer) to perform any function without authority; secures access without authority	any person who knowingly causes a computer **to perform any function** for the purpose of securing access **without authority** to any program or data held in any computer… any person who knowingly **secures access without authority** to any computer for the purpose of obtaining, directly or indirectly, any computer service…

Chinese legislature does not base on 'unauthorised access'; rather, a cybercrime is committed if the actor violates State's regulation.[1034] There is no authoritative interpretation as to what constitutes 'State's regulation' in the cyber context. Thus, the criminal provision regarding 'State's regulations' for all criminal cases subsequently applies, and the provision states that 'State's regulation' refers to all laws and administrative regulations issued by the National People's Congress (NPC), the Standing Committee of the National People's Congress

[1034] Article 285 of the Criminal Law, China.

(SCNPC) and the States Council (SC).[1035] Such a rule suggests that **any** violation of **any** law or regulation issued by these three organs may constitute cybercrime in Chinese legal context, 'the genuine cybercrime' to be precise. 'Access', according to a leading legal scholar, refers to any activity that 'without being empowered or approved by the competent authorities, interfering with data stored on the computer information system through computer terminals'.[1036]

The Explanatory Report of the Convention on Cybercrime provides an explanation of 'access' and 'without right' – the equivalent term to 'access … without authorisation'. 'Access' is referred to as 'the entering of the whole or any part of a computer system',[1037] including hardware, programs and data stored. 'Without right' means 'without authority (whether legislative, executive, administrative, judicial, contractual or consensual)', or 'not covered by established legal defences, excuses, justifications or relevant principles under domestic law'.[1038]

The US struggled with the issue whether an access is 'exceeding authorisation' or 'without authorisation' in judicial practice since the US legislation distinguishes these two. 'Exceeds authorised access' is explained as 'access a computer with authorisation and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter' under the CFAA.[1039] Such access exceeding authorisation happens widely in offences where the offender is an employee: the employee is authorised to use the computer, but not authorised to use the computer in the way they did. However, in the CFAA an explanation on 'unauthorised access' is not provided, and it is thus unclear of what constitutes 'unauthorised access'. Therefore, different tests have been developed to determine whether an access is 'without authorisation' or 'exceeding authorisation', such as the code-based restriction test[1040] of Orin S. Kerr and the *mens rea* test[1041] of David Thaw. Thaw criticised

[1035] Article 96 of the Criminal Law, China.

[1036] Zhang Mingkai, *刑法学* (Criminal law), Beijing: China Law Press, 2011, p. 928.

[1037] Article 46 of the Explanatory Report of the Convention on Cybercrime.

[1038] Article 38 of the Explanatory Report of the Convention on Cybercrime.

[1039] 18 U.S.C. § 1030(e)(6).

[1040] According to Kerr, the code-based restriction test is developed to exam how 'the [computer] owner or her agent codes the computer's software so that the particular user has a limited set of privileges on the computer'. In other words, under this test the owner of a computer has the privilege to decide whether a user can log on to a computer and what that user can do with that computer. Orin S. Kerr, 'Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Act', *Public Law and Legal Theory Research Paper Series Research Paper No. 65*, (2003): 1596-1668.

Kerr's code-based test for failing to cover new forms of computer misuses that the CFAA should cover, cyber bullying for instance.[1042] Thus, Thaw's *mens rea* test covers all crime involving a computer, including hacking (computer as the target) and crimes of the physical world that are made easier by a computer (computer as the tool or as an incidental element), such as searching for victim's information online.[1043]

Comparing these two tests, one can notice that the starting points – the approriate scope of cybercrime, and subsequently, the proper scope of the CFAA – of these two tests are different. Kerr intends to keep the CFAA computer specific, and only the genuine cybercrime should be covered, whereas Thaw prefers to retain all crimes under the CFAA as long as a computer or network is somehow involved. In fact, this divergence mirrors an important issue discussed in the US: what acts should be covered by the CFAA. In other words, the extent to which the CFAA should be cyber-specific. Analysing the offences currently covered by the CFAA, most of them are related to crimes targeting a computer. The only exception is that 18 U.S.C. § 1030(a)(4) criminalises computer-related fraud. Thus, it seems that the legislature at least intends to keep the CFAA covering the genuine cybercrime. However, courts do not agree with the legislators. In the case *US v. Drew*[1044] the court held the defendant guilty of

---

As Thaw commented, Kerr 'proposes that courts interpret the term "access" to be subject to the terms of private agreements governing use, but that the term "(without) authorization" be limited to circumvention of these code-based restrictions'. David Thaw, 'Criminalizing Hacking, Not Dating', *Journal of Criminal Law and Criminology*, vol. 103 3(2013): 907-948, p. 943.

[1041] In the test Thaw proposed a two-part intent requirement:

'(1) that the actor intentionally engages in an action not only constituting unauthorised access, but also that the intent be that the action results in unauthorised access…and

(2) that this action be in furtherance either of one of a list of specifically prohibited computer-specific crimes or alternatively in furtherance of an act otherwise unlawful under existing state or federal law.'

David Thaw, 'Criminalizing Hacking, Not Dating', *Journal of Criminal Law and Criminology*, vol. 103 3(2013): 907-948, pp. 910-911.

[1042] *Ibid*, p. 943.

[1043] *Ibid*, p. 929.

[1044] *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). Drew, a resident of O'Fallon, Missouri, entered into a conspiracy in which its members agreed to intentionally access a computer used in interstate commerce without (and/or in excess of) authorization in order to obtain information for the purpose of committing the tortious act of intentional infliction of emotional distress upon 'M.T.M.', subsequently identified as Megan Meier (Megan). Megan was a 13-year-old girl living in O'Fallon who had been a classmate of Drew's daughter Sarah. Pursuant to the conspiracy, on or about 20 September 2006, the conspirators registered and set up a profile for a fictitious 16 years' old male juvenile named 'Josh Evans' on the www.My Space.com website (MySpace), and posted a photograph of a boy without that boy's knowledge or consent. Such conduct violated My Space's terms of service. The conspirators contacted Megan through the MySpace network (on which she had her own profile) using the Josh Evans pseudonym and began to flirt with her over a number of days. On or about 7 October 2006, the conspirators had 'Josh' inform Megan that he was moving away. On or about 16 October 2006, the conspirators had 'Josh' tell Megan that he no longer liked her and that 'the world would be a better place without her in it'. Later on that same day, after learning that Megan had killed herself, Drew deleted the Josh Evans MySpace account. Drew was charged with one count of conspiracy in violation of 18 U.S.C. §

obtaining unauthorised information by means of using a computer for her cyberbullying activity. This judgement demonstrates the court's position on the reach of the CFAA. It is thus clear that there is not yet a consensus on the proper scope of the CFAA in the US, neither in the academic nor between the legislators and judges.

England does not use the term 'unauthorised access' either. Instead, it adopts the term 'cause a computer to perform any function…unauthorised'. According to the ECMA, 'causing a computer to perform any function' refers to the alteration, erasure, movement, or use of data stored on the computer accessed.[1045] Under this explanation, the crimes clearly target at data. Thus, any electronic intervention that causes changes to the data is cybercrime.

By avoiding defining 'access' and 'authorisation', the ECMA in English law does not need to consider which part of the computer has been accessed – hardware or software – without authorisation. Instead, it can go beyond protecting a computer to protecting the data stored on any given computer. To be clearer, if a person secures access to certain data to which they are not authorised, their act is illegal. In a situation like this, whether they are authorised to use the computer on which the targeted data is stored does not matter. For instance, a person obtained access to a computer and deleted some of the data stored on that computer. If that person was not authorised to use that computer, it does not matter whether the law protects the computer or the data, because in either case that person will have violated the law. However, it happens that a person is authorised to use that computer (for example, to use it to surf online), but is not authorised to delete the data stored on that computer. Issues arise on whether this act is 'without authorisation' or not. Put it in another way, whether this act violates the law or not. Two situations may apply. For the one, if the applicable law protects the data, the perpetrator violates the law because they damaged the data. For the second, if the applicable law protects the computer, does the perpetrator violate the law? They are authorised to use that computer, but abuse their authorisation. This is exactly the issue widely discussed in the US, namely, whether 'exceeding authorisation' belongs to 'without authorisation'. If the answer is yes, the issue subsequently becomes the standards of determining authorisation. In England, such discussion has not attracted much attention since the ECMA essentially protects data.

---

371 and three counts of violating a felony portion of the CFAA, i.e. 18 U.S.C. § 1030(a)(2)(C) and 1030(c)(2)(B)(ii), which prohibit accessing a computer without authorization or in excess of authorization and obtaining information from a protected computer where the conduct involves an interstate or foreign communication and the offence is committed in furtherance of a crime or tortious act.

[1045] Section 17(2) of the Computer Misuse Act, England.

Singapore, as borrowing its relevant criminal provisions from the English law, also adopts the term 'causing a computer to perform any function…unauthorised'. Thus, debate on the relationship between exceeding authorisation and without authorisation has neither arisen widely.

Generally speaking, with respect to 'access' and 'authorisation' in the selected legal regimes, it can be observed that China actually encompasses all of the laws and the administrative regulations. The CoC leaves this to individual nations to decide. The US struggles with whether 'exceeds authorisation' belongs to 'without authorisation' and, ultimately, with how to define 'authorisation' in these two kinds of situations. England and Singapore focus on the authorisation to access data rather than the computer (or part of the computer).

Although the US CFAA distinguishes between 'without authorisation' and 'exceeds authorisation', it still interprets these two broadly enough to cover virtually all crimes which involve the use of a computer. Admittedly, US scholars and judges have discussed and analysed the scope of 'unauthorised access' thoroughly. Nonetheless, they do not discuss it on the same basis. One possible reason is that there is no consistent position, or in other words, approach to draft, amend or interpret the CFAA. When defining a 'protected computer', the US opts for an astonishingly broad approach that covers almost all the computers in the world. When interpreting 'access', Congress applied a narrow approach and ruled that 'access' must be gained to a computer, not to the data held on that computer. Thus, 'exceeds authorisation' is different to 'without authorisation', because the former means the offenders have the authority to use the computer, while in the latter they do not. Thereafter, different tests have been developed and applied to determine in what circumstances the access 'exceeds authorisation' and in what conditions the access is 'without authorisation'. Further, after deciding this, yet more tests have been developed on criteria of determining the authorisation in 'exceeds authorisation' and that in 'without authorisation'. With reference to the English experience, if the CFAA have made clear that it intended to protect data, then 'access' subsequently indicates 'access to data', and 'exceeding of authorisation' does not exist. By doing do, the problem US scholars have struggled with for years can be solved. However, the US hesitates between protecting computers and protecting data, as is concluded in the Chapter on the US.

In sum, the different understanding and positions on 'computer' and 'data' reflect different approaches of interpreting the provisions, and they to a certain degree determine the different experiances of the US and England.

7.2.5.3 'Fault element' of cybercrime: intention, knowledge and recklessness

Comparing with other elements such as 'computer' and 'authorisation', fault element has attracted relatively little academic attention. The limited academic attention has primarily focused on the extent to what 'intention', or 'knowledge' under certain Articles, factors the scope of the genuine cybercrime. Namely, whether recklessness should be a fault element of the genuine cybercrime.

In China, computer crimes must have been committed intentionally or knowingly. This means the offender knew that their act would cause the consequences to happen and did it intentionally, or at least did not take any measure to prevent the consequences from happening.[1046] To be more specific, as long as the actor committed the offence intentionally or knowingly, the *mens rea* element is met. For the case of the CoC, all kinds of the genuine cybercrime must have been committed intentionally. When it comes to the exact meaning of 'intentionally', the drafters left it to national interpretation considering the different situations of the Signatories. In the US, 'intentionally' and 'knowingly' apply to different offences. For instance, under 18 U.S.C. § 1030(a)(1) it is knowingly access to a computer without authorisation and obtained restricted information penalised. In contrast, 18 U.S.C. § 1030(a)(2) states that 'intentionally access a computer without authorisation …' shall be punished. In England, considering the fact that 'mere hacking' is criminalised, the offender does not need to know that their actions will cause certain consequences, a knowledge of the act will cause a computer to perform the function is enough. However, the ECMA does require the offender to know that they are gaining access, and that the access is 'unauthorised'. The same interpretation applies to Singapore.

By comparison, it is mostly intention or knowledge, or both, prohibited, and 'recklessness' and 'inadvertency' seldom apply. The reason for this phenomenon is to limit the scope of criminalisation. As the Law Commission puts it, 'the offence should not become a "catch-all"

[1046] Zhang Mingkai, *刑法学* (Criminal Law), Beijing: China Law Press, 2011, pp. 928-929.

for all forms of irregular conduct involving a computer, but should aim only at deterring the deliberate activities'.[1047] The ERCoC also expresses this purpose.

Be that as it may, one potential problem is, as many cases have shown, that the damage caused recklessly may be far beyond the actor's expectation. For instance, a programmer made a computer virus to test the security of a computer system. The computer system was immediately paralysed and uploaded the virus online. Soon enough, this virus infected and destroyed thousands of computers, including computers used for national security and defence. This consequence is far beyond what the programmer could expect. Considering such situation, the US and England take a step forward by explicitly criminalising 'recklessness' to consequences. The CoC has left the decision to be made at the domestic level. China and Singapore, two jurisdictions that famous for social control and severe punishment, have not yet reflected in their legislations on this very circumstance. As the current practice has shown, whether to criminalise activities that recklessly cause huge damage is a question worth consideration.

7.2.5.4 Examining the scope of cybercrime

The selected legal regimes have endowed various meanings to the abovementioned three elements, 'computer', 'unauthorised access' and 'fault element'. Consequently, the nature and scope of cybercrime vary among the selected legal regimes. This variety can be best illustrated by addressing the legaility of mere hacking. 'Mere hacking' has been widely discussed in all the selected legal regimes.[1048] It refers to situations where the actor hacks into a computer and does not change any data stored on that computer or the setting of it. Whether to criminalise mere hacking is not a simple choice, but a decision made on various considerations. Different positions on whether to and why to criminalise mere hacking demonstrate the approach legal regimes take. For instance, the Netherlands penalises 'mere hacking', meaning that intentionally breaching the security of an automatic device by a technical operation is an offence. On the contrary, in India it is after the offender impairs the system or data stored on a computer that criminal liability would be pursued.[1049]

[1047] The Law Commission, *Computer Misuse No. 186* (1989), [3.27].

[1048] Other issues discussed relateing the scope of criminalisation include, but are not limited to, the criminalisation of aiding and abetting with a computer and the criminal liability of Internet service providers. Considering that these issues are frequently dicussed in one legal regime and not in others, this topic chooses mere hacking to illustrate the diverging scopes of criminalisation.

[1049] Sections 43 and 65 of the Information and Technology Act, India.

It can hardly hold true that China criminalises 'mere hacking'. Article 285(1) outlaws the hacking of computers involved in state affairs, national defence and the most sophisticated science and technology. As for the computers used by individuals and other institutions, a criminal offence is committed only when the offender controls a computer or obtains the information stored on that computer after hacking.[1050] In other words, the hacking itself to individual computers is not a violation of the law, but controlling the hacked computer or obtaining the information is. Thus, for the personal computers in China, it is the obtaining of information or controlling the computer after hacking that prohibited, not the hacking itself. But for computers involved in the listed fields, 'mere hacking' is criminalised, even if the offender only intends to make him 'cool' among his peers by hacking into those computers.

The Convention on Cybercrime criminalises mere hacking. Concerned that 'mere hacking' can provide opportunities for further crime, the drafters of the CoC regard mere hacking as an entrance activity. For instance, offenders can commit fraud after observing the personal information stored on the hacked computer. Thus, if mere hacking is criminalised, further crimes can to a large extent be prevented. In addition, in the Explanatory Report of the Convention, the drafters state explicitly that the conduct of illegal access like hacking 'should in principle be illegal in itself'.[1051] Thus, knowing that outlawing mere hacking represents a broad criminal scope of the CoC, and might be overly broad, the drafters still support the criminalisation of mere hacking.

In the US, there is no complete criminal offence as 'mere hacking'. To be clearer, hacking alone is not treated as a complete and unique cyber offence; rather, it is regarded as an inchoate crime. The US cybercrime legislation, CFAA, does not mention 'mere hacking' specifically. Instead, it states that anybody attempting to commit offences under the CFAA shall be punished. Accordingly, if 'mere hacking' did count as a complete offence, the act of trying to commit it would also be punishable. This could lead to one situation: an actor pushes the power button of a computer with the intent of breaking through its security system, but is caught before the computer starts to work. This actor had committed a crime and shall be pursued criminal liability even though the computer had not yet booted up. To avoid such a situation from happening, 'mere hacking' is regarded as preparation for committing offences.

[1050] Article 286 of the Criminal Law, China.

[1051] Article 44 of the Explanatory Report of the Convention on Cybercrime.

England has penalised ‘mere hacking’ since 1990. Like the drafters of the CoC, English legislators intend to deter further crimes through criminalising ‘mere hacking’. According to section 1(1)(a) of the ECMA, a person is criminally guilty if he ‘causes a computer to perform any function with intent to secure access to any program or data held in any computer’. This statement indicates that if an actor knowingly tries to gain access to *any* program or data, and such an act causes the computer to perform any function, that actor is criminally liable. This provision, as some scholars have argued, protects programs and data – information in another word – and any attempt to gain access to information is criminalised. Accordingly, the offence covered by this provision is not ‘mere hacking’, but ‘hacking for data’. True indeed, it protects data, and a hacker does not need to be targeting any particular data before a criminal liability can be pursued. However, ‘hacking for data’ is exactly what ‘mere hacking’ is. As defined, mere hacking does not change any data or setting of the computer. Thus, it in fact does not do any harm to the computer. Rather, what it harms is the reliability of data stored on computer. For instance, an actor can take a photo of the computer screen and thus damage the reliability of that data without changing it. Therefore, since the ECMA criminalises ‘hacking for data’, it criminalises mere hacking.

Since Singapore borrowed Section 1 of the ECMA for its domestic law, Singapore also criminalises ‘mere hacking’.

Comparing all these legal regimes, the CoE, England and Singapore treat ‘mere hacking’ as a unique and complete crime on the consideration of preventing further crime. On the contrary, China and the US do not regard ‘mere hacking’ as a complete crime but the preparation of cybercrime.

Considering the reasons to the criminalisation of ‘mere hacking’ provided by the CoE and England, an offence as ‘mere hacking’ seems to be a measure that closes the ‘entrance activity’ to cybercrime. ‘Mere hacking’ is the preparation of many further cybercrimes, and such preparation can present enormous potential for damage. For instance, an actor A hacks into a computer that controls traffic lights and leaves that computer without changing anything. The government notices this, but they can neither fix the security weakness exploited by A nor file a case if ‘mere hacking’ is not a criminal offence. Later, A once again hacks into this computer and destroys the program controlling the traffic lights. The roads are paralysed, and hundreds of people are injured or even killed. If ‘mere hacking’ was a criminal

offence, as is the case with the CoE, England and Singapore, measures would have been taken right after A's first hacking, and then the later tragedy could be avoided.

In addition, the police and prosecutors often encounter difficulties when collecting evidence and proving a cybercrime, and criminalising mere hacking can under certain circumstances lower the burden of proof. For instance, it commonly happens that the police cannot gather enough evidence proving the computer is impaired or the data is damaged. In this situation, the prosecutor can charge the actor with mere hacking since under this offence it is not necessary to prove the actor caused noticeable damage to either computer or data.

Furthermore, such an offence informs the 'netizens' that unauthorised access to computers is not allowed. Therefore, firstly, their own computers are protected from being hacked, and secondly, they should not hack into the computers of others.

7.2.6 The function of computer and the security of data: two different legal interests

By the above comparisons, one factor surfaces as a key element behind the discussions: the two different subjects threatened by cybercrime and protected under relevant legislation - computer and data. The different positions of legislations on computer or data do not only contribute to determining the scope of cybercrime. Moreover, they lead to different issues a jurisdiction encounter when legislating against cybercrime and adjudicating relevant cases. For instance, the inability of distinguishing computer and data results in the difficulty of defining computer, and it further leads to the different experiences when interpreting 'unauthorised access' in the US and England.

Chinese legislation on cybercrime, as stated by Chinese scholars, protects the security of computer information systems and data. However, the meaning of 'the security of computer information system and data' remains untouched. According to Chinese legislators and scholars, Article 285(1) of the Chinese Criminal Law prohibits hacking into a computer information system involved in state affairs, national defence and the most sophisticated technology, and thus protects the security of any such computer information system. Article 285(2) of the Chinese Criminal Law, which prohibits control over a computer information system or obtaining data after hacking, protects both the security of the computer information system and that of data. Comparing these two Articles from the perspective of the prohibited behaviours, the former can be seen as 'mere hacking', which threatens the confidentiality and reliability of the data stored on the computers involved in the listed fields; while the latter

impairs the data processing capability of the hacked computer and the integrity of data stored on it. Therefore, although both Articles 285(1) and (2) protect the security of computer information system and data, the term *security* in fact refers to different things.

In contrast with the unclear connotation of 'the security' in China, the Convention on Cybercrime states explicitly that offences under Title 1, Section 1, i.e. the genuine cybercrime, have all been established to protect the confidentiality, integrity and availability of the *computer system* and *data*. Further, the CoC makes it clear that the confidentiality, integrity and availability of data are distinguished and independent from those of computer systems by prohibiting different behaviours in different provisions, irrespective of the confusions raised by the ERCoC.[1052] To put it in another way, an actor can damage the confidentiality, integrity and availability of data without damaging the availability of computer systems. For instance, under Article 4 of the CoC a person commits a cybercrime if he intentionally damaged data without right. This Article mentions nothing about whether this person damages the function of computer. It implies that under this offence whether the function of computer is interfered is immaterial. As long as the data is damaged, criminal liability shall be pursued. On the contrary, if a person intentionally hindered the function of a computer system *without right*, he violates Article 5 of the CoC. Admittedly, under Article 5 the actor must hinder the function of computer system through inputting, transmitting or other operation of computer data, and thus the data is changed. However, the wording of this article in fact suggests that the change of computer data under this offence can be done *with right*. This indicates that the change of data can be lawful, but the interference of computer system is unlawful. For instance, under one form of DoS attack, the offenders hinder the function of the targeting computer through sending a large quantity of emails to an email server. Subsequently, the email server responds slowly and finally stops working. In a case like this, the offender has the right to send emails. However, he does not have right to interfere the function of the server.

In the US, the protection of computers and data lacks consistency. On the one hand, it seems that the US recognises that computers and data are different by prohibiting the act of trafficking data that could be used to hack into a computer. On the other hand, the hacking offence does not distinguish between the security of computer and the security of data, similar to Chinese legislation. According to 18 U.S.C. § 1030(a)(1), an offence has been committed if

[1052] For the confusions presented by the ERCoC, see Chapter 3 The Convention on Cybercrime of the Council of Europe.

the offender hacked into the computer and obtained information stored on it. Given the fact that this section protects the security of computer, and there is no single Article only protecting the data from being obtained or damaged, the conception of the security of data is dependent on the conception of the security of the computer in the US context.

The legislation on cybercrime in England treats computer and data differently and regards data as its fundamental. In other words, in England offenders can damage one without damaging the other – an opposite position to that of the US. For instance, section 1 of the ECMA criminalises unauthorised access to computer material, data in another word; yet section 3 penalises unauthorised acts with intent to impair, or with recklessness as to impairing computer. Comparing these two sections one can see that while section 1 protects data, section 3 protects computer.

Singapore, given the fact it borrowed its SCMA mostly from the counterparts in England and Canada, has adopted both of their positions, i.e. protecting both computer and data. Sections 3, 4 and 5 of the SCMA, like their equivalents in the ECMA 1990, focus on the confidentiality, integrity and availability of data.[1053] On the contrary, section 6 is borrowed from Canada, and focuses on computer service. Section 6 rules explicitly that whoever knowingly intercepts any function of computer or secures access for obtaining computer service shall be punished. Thus, it can be concluded that the SCMA distinguishes data and computer: sections 3, 4 and 5 are enacted to protect data, and section 6 to protect the function of computer.[1054]

Comparing all these jurisdictions and the CoE, it can be observed that by roughly saying they protect the security of computer, they in fact protect different objects – computer or data. Therefore, the term 'security' refers to different qualities of the computer and data, such the capability to process data of the computer under the Chinese CL and the confidentiality of data under the CoC. Then, what exactly do the 'security of computer' and the 'security of data' mean?

[1053] The original section 3 of the England Computer Misuse Act was enacted in 1990 to protect data. In 2006 the England Police Justice Act amended section 3, and from then it takes computer into the coverage. Section 5 of the Singapore Computer Misuse Act was drafted before 1993, in which period section 3 of the ECMA was not changed and still protected data. Learning from the original section 3, section 5 of the SCMA protects data.

[1054] For detailed analysis on the appraoch taken by Singapore, see Chapter 6 Cybercrime Legislation in Singapore. See e.g. Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', *Singapore Journal of Legal Studies*, (1994): 263-331. See also Katherine S. Williams and Indira Mahalingam Carr, 'The Singapore Computer Misuse Act – Better Protection for the Victims?' *Journal of Law and Information Science*, vol. 5 2(1994): 210-226. See also Jonathan Clough, 'Data Theft? Cybercrime and the Increasing Criminalisation of Access to Data', *Criminal Law Forum*, 22(2011): 145-170.

For the 'security of computer', computer is protected for its function of data processing, and also data storage and communication in the US context. Thus, the security of a computer refers to the security of data process, and may also include the security of data storage and communication. The security of data process suggests that a computer performs certain functions through processing data, and that such functions can proceed normally. The security of data communication can be understood in a similar way, that the function of communicating data runs normally, i.e. the inputting and outputting of data run normally. However, the meaning of the security of data storage is unclear. Does it refer to a computer being able to store data normally, or does it refer to the data stored on a computer is secure? Apparently the security of data storage should refer to the function of storing data working normally. Otherwise, it would encompass or overlap with 'the security of data', which seems unreasonable since a computer is in fact a carrier of data, not the data itself. Through this analysis, it becomes clear that the security of a computer refers to its functions, including data processing, data communication and data storage, working normally.

For the 'security of data', as the CoC has identified, it means the confidentiality, integrity and availability. Data itself has no function, but it is the carrier of information. Considering that the information must keep confidential and reliable, especially the classified information, the data that delivering information must keep confidential and unchanged.

Reading the connotations of 'security of computer' and 'security of data' in conjunction with 'mere hacking', the divergence between protecting the function of computer and the confidentiality of data can be identified. By the definition of mere hacking, it does not impair the data stored on the computer or interfere with the functions of that computer. What it impairs is the confidentiality of data, because even if the 'mere hacker' did not add, delete or copy the data stored on the hacked computer, the data is no longer confidential or reliable. This analysis is supported by the fact the England criminalises 'mere hacking', while China and the US do not. The ECMA focuses more on data, and since 'mere hacking' threatens the confidentiality of data, it is criminalised. In contrast, neither China nor the US explicitly states in their legislation that data is protected independently. For both of them, only if the function of a computer is damaged, the act shall be criminalised. Thus, since not damaging the function of computer, 'mere hacking' is an offence in neither of them.

In sum, it can be observed that, apart from the previously analysed and compared three elements of cybercrime, i.e. 'computer', 'unauthorised access' and 'fault element', the interest

protected by the legislation on cybercrime can also, to a large extent, determine the scope of the legislation. On the basis of the previous three elements, the interest protected may perform a more significant role in determining whether an act is a cybercrime under relevant legislation.

7.2.7 Inadequacy of the existing jurisdiction principles over cybercrime

It is widely recognised that jurisdiction over cybercrime is a thorny issue. As is demonstrated by jurisdiction principle adopted in the selected countries[1055] and the CoE, territory is the central factor in deciding jurisdiction despite the non-physical nature of the bits and bytes that constituting cybercrime. However, facts show cybercrime is not bound to territory, and thus the principle of territory appears less sufficient and adequate. Solutions to this insufficiency attract scholarship around the world, and numbers of measures have been proposed, such as alternatively adopting extra-territorial jurisdiction or personal jurisdiction. However, none of the jurisdiction principles has been applied adequately or sufficiently.

Specifically, 'location' still serves as a major factor to decide cybercrime jurisdiction since territorial principle is the main jurisdiction principle.[1056] However, 'location' is not a simple topic when the crime in question involves the use of computer and network. According to national legislations, the selected countries may claim jurisdiction if the act is committed within their territory, if the effect is felt within their territory, or the actor is in their territory when the act is committed. For instance, according to the ECMA, England can claim jurisdiction if the location of the act, the targeted computer, or the actor is in its territory,[1057] and so can Singapore.[1058] The CoE also adopts the location of act as its primary factor in deciding jurisdiction.[1059] However, with respect to cybercrime, none of the location of the act, the effect, or the actor is clear. For the case of the act, the absence of substantive criminal law especially presents challenges on the issue whether to prosecute or convict an act which is illegal in one country yet not in another. As Susan W. Brenner and Bert-Jaap Koops put it,

---

[1055] Under 7.2.7 'country' is used instead of jurisdiction in other parts of this research, to avoid confusions between jurisdictions as an area or a country, and jurisdiction as an authoritative right over cases, irrespective of the fact that Engalnd is not a country.

[1056] See e.g. Susan W. Brenner and Bert-Jaap Koops, 'Approaches to Cybercrime Jurisdiction', *Journal of High Technology Law*, vol. IV 1(2004): 1-46, p. 44.

[1057] Sections 4 and 5 of the Computer Misuse Act, England.

[1058] Article 11 of the Computer Misuse Act, Singapore.

[1059] Article 22 of the Convention on Cybercrime, the Council of Europe.

> '[i]n one recent case, a French court assumed jurisdiction over Yahoo, an American online content provider, and ordered it to remove web pages showing Nazi memorabilia, material that is illegal to view in France but legal almost everywhere else. In another case, a British court held a British subject liable for posting photographs on an American web server considered obscene in Britain but not in the United States. Still another, an American court held the president of a gambling company organised and headquartered in Antigua liable for soliciting and accepting bets from Americans over the Internet.'[1060]

Moreover, the act of committing cybercrime is an on-going process, thus it is difficult to decide the location of the act. For instance, in the above case that a British national uploading obscene photographs on a US hosting server, the uploading act started in Britain, went through the network of many countries, and terminated in the US. This case takes place partly in Britain and partly in the US, and thus it is unclear which country is the location of the act.

For the case of the effect, firstly, an attack launched in the US to Singapore may go through Chinese network. Subsequently, Chinese network server experiences some change. There is no consensus on the issue whether such change counts to 'effect'. Thus, there is no consensus on the issue whether in such a condition China has jurisdiction over the case. Secondly, the effect of a cybercrime may be felt in dozens of countries, as the virus 'love-bug' infected and damaged computers in more than twenty countries. Such situations inevitably raise jurisdiction conflicts under the territorial principle. The location of the actor is not easy to identify either. There is a particular situation where the actor committed the offence in country A yet he is the national of country B, and B for some reason does not extradite him to country A.[1061] The reasons can be there is no bilateral or multilateral treaty on judicial assistance, country A may punish the perpetrator in an inhuman way, and others.[1062]

In this regard, some countries adopt the extra-territorial jurisdiction instead of territorial principle, such as the US. The extra-territorial jurisdiction in the US means that it can exercise jurisdiction over acts committed upon a 'protected computer', which is defined to encompass all computers in the world as long as they are connected to the Internet or an

[1060] Susan W. Brenner and Bert-Jaap Koops, 'Approaches to Cybercrime Jurisdiction', *Journal of High Technology Law*, 1(2004): 1-46, pp. 10-11.

[1061] Susan W. Brenner and Bert-Jaap Koops, 'Approaches to Cybercrime Jurisdiction', *Journal of High Technology Law*, 1(2004): 1-46, pp. 16-19.

[1062] *Ibid*.

inter-state network.[1063] By this way, the US could deal with a situation where no country claims jurisdiction.[1064]

Considering the borderless character of cybercrime, the extra-territorial principle might be the future of cybercrime jurisdiction. However, this assumption is proved to be wrong. The extraterritorial jurisdiction is in its essence 'the ability of a [country] to punish acts of foreign individuals or legal entities'. This is exactly what the debate on such jurisdiction is – whether, and on what occasions if so, a country can apply its standards to foreign persons who are not its nationalities.[1065] The territorial jurisdiction authorises a country to regulate acts conducted on its territory, as long as the acts took place in the territory of the country in question, even when these acts have been carried out by foreigners.[1066] Such an assertion of judicial power is commonly accepted, because it is based on reasonable grounds - the location of the act committed, as pointed out by Professor Cedric Ryngaert.[1067] The 'significant link' suggested in the ECMA also reflects this rationale. However, the extraterritorial jurisdiction sometimes lacks the reasonable link. For instance, on the basis of jurisdiction principle established by the CFAA, the US can claim jurisdiction as long as an actor has affected 'interstate or foreign commerce or communication'. Considering the Internet is an instrument of interstate commerce and communication, the US can exercise jurisdiction over actors who have affected the Internet or the computers that connecting to the Internet.[1068] Under this jurisdiction, the link is not the location, the nationality or others, but is a computer connected to the Internet, which is neither 'reasonable' nor 'significant'. Facing this problem, the issue of adopting extra-territorial principle subsequently becomes on what occasions connection between crime and jurisdiction is significant and reasonable. Cedric Ryngaert does not provide a clear answer or criteria to this question. Another scholar, Sir Ian Brownlie, offers some clues, indicating that such connections should be

1) substantial and bona fide;

[1063] For details of the 'protected computer' and the extra-territory jurisdiction in the US, see Chapter 4 Cybercrime Legislation in the US.

[1064] Susan W. Brenner and Bert-Jaap Koops, 'Approaches to Cybercrime Jurisdiction', *Journal of High Technology Law*, vol. IV 1(2004): 1-46

[1065] Laurent Cohen-Tanugi, 'The Extraterritorial application of American Law: Myths and Realities', February 2015, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2576678. Last visited October 2015.

[1066] *Ibid*.

[1067] Cedric Ryngaert, *Jurisdiction in International Law*, Oxford: Oxford University Press, 2015.

[1068] For details of the US jurisdiction over cybercrime cases, see Chapter 4 Cybercrime Legislation in the US.

2) the assertion of jurisdiction should not intervene in the jurisdiction of other states; and

3) the jurisdiction should be based on accommodation, mutuality and proportionality.[1069]

Some countries have turned to the nationality principle for help, such as England. The nationality principle in cyber cases means when the nationals of a country commit cybercrime, the country can claim jurisdiction. For example, the newly introduced Serious Crime Act 2015 in England establishes the national principle for deciding jurisdiction of cyber cases. Under this principle, if the perpetrator was a United Kingdom national when they committed the act, and this act also constituted an offence according to the law of the country in which this act took place, England can claim jurisdiction.[1070] The Convention on Cybercrime also establishes the nationality principle as an optional principle for individual States.[1071] However, the nationality principle also raises issues. It may be impossible to decide which country has the jurisdiction to launch the investigation in a given case, because the nationality of the offender is often unknown.

The nationality of the victim would lead to another discussion, that many countries could claim to have jurisdiction because a cybercrime may have thousands of victims and they can be scattered worldwide. Under this situation, new tests or creteria need to be developed to decide which of the countries has the priority to exercise jurisdiction before the nationality of the victim can help.

Some other jurisdictions may also be applicable, such as protective jurisdiction and universal jurisdiction. For instance, China establishes these two as alternatives to territorial and personal jurisdictions. However, both of them face the problem of to what extent the connection between a case and jurisdiction is 'reasonable', as discussed above with regard to the extra-territorial principle. In common with the situation as regards the territorial principle, many issues must be addressed before other principles can be applied to cybercrime.

[1069] For details see Chapter 6 Cybercrime Legislation in Singapore. See also Ian Brownlie, *Principles of Public International Law* (6th edition), Oxford: Oxford University Press, 2003, p. 309.

[1070] Section 5(1A) of the Computer Misuse Act, England.

[1071] Article 22 of the Convention on Cybercrime, the Council of Europe.

7.3 Conclusion

The central objectives of this research are (1) to explore and compare legislative arrangements of other selected legal regimes, with an aim to generalise and develop possible solutions to cybercrime, and (2), based on the legislative approaches against cybercrime in China and its practices, to propose recommendations upon which the criminal law can be improved. After the preceding investigation and comparison on the cybercrime legislations in the selected legal regimes, four aspects are to be addressed in order to answer the central research question: how the criminal law can be adapted to regulate cybercrime.

7.3.1 The necessity of cyber-specific legislation

The first important aspect of the central research question is whether a cyber-specific legislation is necessary to regulate cybercrime, and the answer is, on the basis of this research, yes. Before acknowledging the necessity for cyber-specific legislation, all the selected jurisdictions applied the then existing criminal provisions to cybercrime. However, the application of these existing criminal provisions to cybercrime caused more problems than it could solve, and the necessity for cyber-specific criminal law was thus recognised.

In the early days of legislating against cybercrime, the selected jurisdictions limited the scope of these cyber-specific laws on purpose, either because they intended not to infringe the online freedom and privacy or they did not realise the serious harm cybercrime could cause. As information technology developed, followed inevitably by the development of cybercrime, these intentionally limited laws were proved insufficient to deal with the wrongdoings it intended to tackle. Therefore, amendments to cybercrime legislations have been made.

For the first, new forms of cybercrime appeared and challenged the cyber-specific law. Consequently, the selected jurisdictions were obliged to amend their legislation on cybercrime so as to cover the gaps presented by new forms of cybercrime in the decades following.

For the second, the threat to national security raised by cybercrime becomes a major concern for all the selected jurisdictions. As the increasing involvement of computer and network in vital sectors such as national defence and public emergency system, the potential to manipulate computers to launch attacks arises. In addition, the previously introduced cyber-specific offences had not successfully deterred cybercrime and in the following years cybercrime became increasingly common and severe. Considering these two aspects, more

offences have been introduced, more powerful enforcement measures have been taken, and heavier punishments have been established; all to deter cybercrime, particularly that which targets national security.

As a conclusion, from the above convergences in promulgating and amending the cyber-specific legislation, one can notice that the necessity of the legislation is not limited to promulgation. More importantly, the cyber-specific legislation should be reviewed and updated constantly. This necessity indicates two perspectives of legislating against cybercrime. Firstly, eventhough when a new form of cyercrime appear, its constituting elements are not always evident or clear, and for most occasions the constituting elements are always not evident or clear, legislators still need to respond to this new form in order to tackle it. Secondly, the initial responses to the new form of cybercrime may prove to be inadequate in the later period, and therefore, constant reviews and updates on the resposes are also necessary.

7.3.2 The advantages and disadvantages of legislative approaches in the selected legal regimes

The unsuccessful attempts of using traditional criminal law and the subsequent alike enactment of cybercrime legislations in the selected jurisdictions and the CoE indicate the necessity of legislative responses to address cybercrime issue. However, the extent to which these responses are adequate and systematic cannot be assessed with mathematical precision.[1072] Taking the perspective of one of the comparison topics above – the distinguished computer and data, three approaches of the legislative responses can be identified, namely, protecting the function of the computer, protecting the security of data, or protecting both. Different positions on the interests protected by cybercrime legislation represent different answers to Aspect 2, the adequate and systematic approaches the legal response can take. Namely, if a legal regime protects the security of data, the DoS attack may not be cybercrime, since it only damages the function of a computer in most instances. In contrast, if a legal regime protects the computer, then 'mere hacking', given that it only damages data, is not cybercrime.

The first approach is the one taken in China and the US: protecting the function of the computer (hereafter the computer approach). Take the US CFAA as an example. Under the

[1072] Douglas H. Hancock, 'To What Extent Should Computer Related Crime be the Subject of Specific Legislative Attention?' *Albany Law Journal of Science and Technology*, vol. 12 (2001): 97-124.

CFAA, the function of the computer includes the capability of data processing, data storage and data communication. In this regard, the CFAA protects the computer from being damaged or manipulated to perform a function that it would not normally do or not intended by the owner. However, in practice, data has increasingly become one of the targets of cyber wrongdoings. Therefore, in order to regulate the cyber wrongdoings which threatening the security of data, data has been treated as the computer in judicial practice. To be clearer, according to the definition, the computer is a data processing device that 'performing logical, arithmetic, or storage functions'.[1073] Thus, the function of data storage is a part of data process. Since data process function is protected, the data storage function is also protected. The data storage function in fact contains two perspectives: one is the functionof the computer to store data, and the other is the data stored on the computer. Accordingly, 'the function of data storage is secure' also contains two perspectives: one is the data storage function can work normally, and the other is the data stored on the computer is secure. Through doing this, the function of computer is interpreted to include the security of data, and the protection of data is dependent on the protection of the computer. To give an example, on the reasoning that if the data stored on a computer is damaged, the function of that computer is subsequently damaged, subsection 18 U.S.C. § 1030(e)(8) defines 'damage' to include 'any impairment to the integrity or availability of data, a program, a system, or information'. Consequently, the CFAA can apply in cases where data has been damaged. This reasoning process is exactly what the US has done to tackle crimes that involve the damaging of data. In the case *United States v. Mitra*[1074] judges have stated that the provisions against hacking offences protect the function of the computer, and thus convicted the defendant under 18 U.S.C. § 1030(a)(5). However, in another case *United States v. Lloyd*[1075] judges convicted the defendant under the same offence, even though no direct damage was caused to the computer, but only to the data stored on the computer.

[1073] 18 U.S.C. § 1030(e)(1).

[1074] See e.g. *United States v. Mitra*, 405 F 3d 492 (7th Cir 2005). In this case the defendant used radio hardware and computer equipment to send signals to a communication system. His behaviour prevented the system from receiving essential communications for emergency services. During the trial the prosecution and the defence contested whether the defendant had impaired the normal function of the system, in other words, whether the function of a computer was impaired. The defendant was convicted under subsection (a)(5).

[1075] See e.g. *United States v. Lloyd*, 269 F.3d 228 (3rd Cir. 2001). In this case the defendant, after being fired from his company, used a previously set up computer bomb to delete important files and programs stored on the company's computers, resulting in a huge loss of sales and contracts. In the end, the Third Circuit Court concluded that the defendant was guilty of computer sabotage under subsection (a)(5).

The advantage of the computer approach is that for the new forms of cybercrime that targeting the function of the computer, the DoS attacks for instance, no special provision is required. However, there are disadvantages to this approach. Firstly, it leads to the discussion on 'exceeding authorisation', the high degree of reliance on the term 'computer', and the broad interpretation of the function of the computer when criminal acts impair the data stored on computers without damaging computer. Secondly, the protection of the function of the computer indicates that the computer is protected as property – which is also threatened by traditional crimes. It thus may cause confusions between damaging the function of computer through technical means, i.e. the genuine cybercrime, and damaging the function of computer through violence. In other words, it may present problems to the legislators when determining the extent to which the cybercrime legislation should reach – what the US and China are struggling with currently[1076] – and may also present problems to judges when applying relevant provisions.

The second approach is the one taken in England before the EPJA 2006, which focuses on data (hereafter the data approach). In contrast with the computer approach, the protection of a computer in England before 2006 relied on the protection of data. To be clearer, if the computer system has been damaged, the data, on which computer system is programmed and operated, must also have been damaged or impaired. Judging from the fact that England adhered to this approach from 1990 to 2006 without any amendment, a long period in the legislative process against cybercrime, this approach must have worked well during that period. However, wrongdoings that only damaging the function of computer appeared, such as DoS attacks. If the same approach was to be continued, some expansion of the 'security of data' was necessary, so that it could contain the 'security of computer'. For instance, in a common kind of DoS attack – sending quantities of emails to the victim so as to impair his computer, emails are processed in the form of data. If quantities of emails are sent to a computer, a large amount of data is sent to that computer. Therefore, the data stored on that computer are changed, and the security of data is damaged. Besides, the computer itself records the time of receipt and other information about emails, and such information is stored in the form of data as well. If emails are sent to a computer, new data is added to what have already stored on the computer, and therefore, the data stored on computer is damaged. Such

[1076] For the details on how China and the US struggle with the issue 'the extent to which cybercrime legislation should be cyber-specific', see Chapter 2 Cybercrime Legislation in China and Chapter 4 Cybercrime Legislation in the US.

an understanding of computer and data can make sense, and it is most likely to apply to future changes in cybercrime because strictly speaking all computer materials are stored in the form of data and all computer information is also recorded in the form of data.

However, under this understanding **any** interaction with a computer can in fact change the data stored on the computer, thus such an interpretation may lead to over-criminalisation. For example, switching on a computer can produce data that records the time the computer was powered up, and by doing so the data is impaired. To prevent this from happening, one possible measure to restrict the criminalisation would be to grant judges judicial discretion to determine whether an act represents a crime or not. Nonetheless, this countermeasure is contrary to the current position in England as regards the capacity of judges. Thus, the data approach has been abandoned in England and replaced by the protection of both of the function of the computer and the security of the data - the third approach.

England (since 2006), Singapore and the CoE take the approach of protecting the function of the computer and the security of data at the same time (hereafter the computer and data approach). Among these three legal regimes, the approach of Singapore is slightly different from that of England (since 2006) and the CoE. Singapore, having borrowed its cybercrime legislation from England (before 2006) and Canada, somehow confuses the acts provisions intend to penalise and introduces different provisions penalising same acts.[1077] This confusion could have been avoided to a large extent if Singapore had devised some way to distinguish between actions threatening the function of the computer and those threatening the security of data, as has been done in England (since 2006) and the CoE.

The application of the computer and data approach has three components. Firstly, identify and distinguish that both the security of data and the function of the computer are the targets of the genuine cybercrime, and recognise the need for protection from legislation. Secondly, each provision must state explicitly the interest it intends to protect in order to avoid confusion between the acts provisions aiming at. Thirdly, when applying and interpreting the legislation, judges must identify the subject impaired, i.e. the function of the computer or the security of the data, and then choose the provision correspondingly. Through sticking to this

[1077] Sections 3-5 of the SCMA are borrowed from the ECMA, and protect the security of data; while section 6 is borrowed from Canada cybercrime legislation and protects computer service, in other words, the function of computer. These two approaches do not necessarily contradict, and they can be merged together as the third approach. However, Singapore confuses the relationship between these two approaches, and uses them to punish same or similar acts. Therefore some scholars argue that these two approaches appear redundant in the Singaporean legal context. For more details see Chapter 6 Cybercrime Legislation in Singapore.

approach, judges can follow the legislative guidance when interpreting relevant provisions, and avoid interpreting computer or data overly broad. The fact that no amendment has been made to adjust this approach since 2006 in England or to the CoC also serves to demonstrate the sustainability and adequacy of this approach.

However, the computer and data approach also has its disadvantages. Considering that the idea behind protecting the function of the computer implies treating the computer as a property,[1078] activities that damaging a computer through technical means appear similar to activities that damaging a computer through violence, such as destroying it with a hammer. Thus, the criminal provisions that protect property are arguably applicable to activities that threaten the function of the computer, just as they apply to activities that threaten devices with other functions, such as televisions. Consequently, the discussion on cybercrime goes back to the question that has long been discussed: whether there is a category as cybercrime, or cybercrime is just traditional crimes committed in new ways.

To answer this question, one must trace back to the act that triggers this question again: the acts that threatening the function of the computer, DoS attack to be specific. Considering the divergence of computer and data, the current genuine cybercrime can be divided into two subgroups: the subgroup threatening the function of computer, and the subgroup threatening the security of data. The latter is the genuine cybercrime that needs new and specific legislation because the security of data is not protected under traditional criminal provisions. The problem is presented by the former, the subgroup targeting the function of the computer: do the acts threatening the function of computer belong to cybercrime, as the jurisdictions and the CoE currently maintain, or they are just traditional crimes committed in new ways.

By answering this issue differently, two routes may apply. The first route is to treat crimes threatening the function of computer as traditional crimes. Thus, the use of information technology to such crimes is like the use of gun or knife to murder: information technology performs as criminal tools. Under this route, computer is protected as property by traditional criminal provisions, and only crimes threatening data are the genuine cybercrime and needs new and specific legislation. Thus, the data approach discussed above can apply, and applied well before being stretched to cover the function of the computer. The second route of solving this problem is to distinguish crimes using information technology threatening the function of computer from crimes using violence threatening the function of computer. Under this route,

[1078] For details of this reasoning see Chapter 6 Cybercrime Legislation in Singapore.

the use of information technology is a factor that differentiates two ways of damaging the function of computer, and under this route the computer and data approach applies.

From the above analysis and comparison, three approaches against cybercrime can be identified with respect to the interests protected by the legislation. The approach focusing on the function of computer, as illustrated by China and the US, may lead to over-criminalisation and raise confusions between provisions against cybercrime and provisions against traditional crime. The approach focusing on the security of data can apply. However, the precondition of the data approach applies is that crime threatening the function of computer is not regarded as the genuine cybercrime and thus not necessarily to be covered by the cyber-specific legislation. This route contradicts the prevailing practice, and therefore appears less adequate. In this context, the approach focusing and distinguishing computer and data is developed and adopted, both by jurisdictions such as England and by organisations such as the Council of Europe.

Therefore, as the answer to Aspect 2, the computer *and* data approach is the most systematic and appropriate one among the three approaches based on the analysis and comparison of this research.

7.3.3 The time for fresh thinking on the jurisdiction issue

The answer to Aspect 3, a sufficient and appropriate jurisdiction principle, may appear disappointed: the traditional principles of jurisdiction all appear problematic in the context of cybercrime, and this issue may continue to raise problems. Some scholars have concluded that the assertion of jurisdiction on cybercrime can be based on the *location* of the activity, where the activity was committed or where the consequences happened, or on the *nationality* of the perpetrator or victim, or where the computer system or database in question is located.[1079] However, as analysed, these choices are not adequate in a cyber-context. The borderless nature of cybercrime, coupled with its multi-victim characteristic, makes it hardly possible to determine the location of either the activity or the damaged computer system or database. The nationality of the perpetrator cannot normally be identified until an investigation has been launched. The fact that one single cybercrime may have thousands of victims complicates the nationality of the victims. Indeed, the extra-territorial principle may

[1079] See e.g. Cristos Velasco, 'Cybercrime Jurisdiction: Past, Present and the Future', *ERA Forum*, Springer Berlin Heidelberg, vol. 16 3(2015): 331-347.

apply on the basis of protective jurisdiction or universal jurisdiction. However, the extent to which the extra-territorial principle can be applied needs much more analysis than scholars currently have. In this context, it is now the time for legal scholars and legislators to apply some creative thinking to the principle of jurisdiction with regard to cybercrime.

7.3.4 The Convention on Cybercrime as an international legal standard against cybercrime

As concluded previously, the legislations against cybercrime taken by the selected jurisdictions and the CoE can be generalised as three approaches. The question arises on which of the three is the most adequate one to apply. Considering a consensus among jurisdictions that cybercrime is a phenomenon cannot be tackled successfully without international harmonisation, the Convention on Cybercrime can perform as an instrument to provide some insights and criterion on this question. That is the answer to Aspect 4 - what is the role of the CoC in shaping appropriate legislation and fostering international cooperation against cybercrime.

Firstly, the CoC adopts the computer and data approach generalised previously to tackle cybercrime. Admittedly, it is difficult to evaluate mathematically and compare the pros and cons of the three approaches. Nonetheless, the adoption of the computer and data approach demonstrates the acceptance and the approval from the Council of Europe. More importantly, it indicates the promotion on this approach from the Council of Europe.

Secondly, following the first argument, it is easier to sign and ratify the CoC if a jurisdiction keeps pace with the Council of Europe, in this case, adopts the computer and data approach. For instance, Article 5 of the Convention criminalises DoS attack through stating that each party shall establish a criminal offence that 'committed intentionally, the serious hindering without right of the functioning of a computer system'. Indeed, Article 5 does not request the parties to establish an exactly the same cyber offence as the genuine cybercrime. Nonetheless, judging from the context, Article 5 is categorised under Title I of Chapter II - offences against the confidentiality, integrity and availability of computer data and systems, it is reasonable to conclude that the drafters of the CoC regard acts hindering the function of computer as a form of the genuine cybercrime. Thus, if a jurisdiction adopts the data approach and does not criminalise the acts prohibited by Article 5, or does not regard it as cybercrime, problems may rise when the jurisdiction implement the CoC into domestic law. Therefore, considering the position taken by the CoE, the computer and data approach is more suitable for a jurisdiction

if it intends to become a party of the CoC so as to enhance the global harmonisation on this very issue.

Thirdly, apart from introducing the framework of cyber offences, the CoC also establishes a mechanism of international cooperation on investigating, prosecuting and deterring cybercrime. It not only requires Parties to enact procedural laws on expedited data preservation, search and seizures, and data gathering; moreover, it harmonises international cooperation issues as regards to cybercrime, such as extradition, mutual assistance and a 24/7 Network for immediate assistance.

7.4 Recommendation to China

Based on the previous comparison and conclusion, this part addresses China specifically on how China can benefit from this research. As concluded in the Chapter on China and in 7.3 Conclusion, the protection of data in China is relying on the protection of the computer,[1080] and the approach reflected in the Amendment (IX) 2015 contradicts the original approach the Criminal Law once took against cybercrime.[1081] Due to these two issues, the scope of criminalisation in China has been expanded, and confusions arise between cyber-specific criminal provisions and traditional criminal provisions. Against this context, the following recommendations are proposed, mainly to systemize the legislative approach China takes in its criminal law. Namely, they are provided to enhance cyber security, and meanwhile to reduce the infringement upon online freedom and avoid over-criminalisation. Together, they hope to contribute to a better regulatation on cybercrime in China.

(1) Efforts should better be given to identifying constitutive elements, rather than defining cybercrime.

The efforts on defining cybercrime will for a great possibility end with no gains, as the last three decades have shown. Moreover, it seems a definition will cause more problems than it could solve. Thus, the efforts on defining cybercrime appear less necessary. Learning from the experiences of the selected jurisdictions and the CoE, legislators and scholars would

[1080] For the information on how China protects data and how it incriminates activities that damaging data, see 7.3.2. The advantages and disadvantages of legislative approaches in the selected legal regimes.

[1081] Before the Amendment (IX) 2015 China took the 'two points and one dimension' approach. It refers to the legislative approach that firstly the legislators distinguish the new crimes targeting computer and traditional crimes facilitated by computer, and secondly within the new crimes targeting computer the legislators distinguish the crimes obtaining information or controlling computer and the crimes interfering computer. For the detailed information see Chapter 2 Cybercrime Legislation in China.

better make efforts on the constitutive elements of cybercrime, namely, the elements that make cybercrime distinguished from other crimes. In this process, the roles computers play in crimes and the interests threatened by cybercrime can help to determine cybercrime to certain degree, and more elements are waiting to be identified.

(2) China can keep the cyber-specific provisions in the Criminal Law, but should review and adjust the provisions in accordance with the development of information technology.

As concluded above, the cyber-specific criminal provisions and amendment to them are necessary. Moreover, the form of these provisions, i.e. either in the CL or as a specific Act, does not matter to a substantial degree, as long as the genuine cybercrime and the traditional crimes facilitated by computers are treated as two separate types of crime. Traditional criminal provisions are drafted before the appearance of cybercrime, and thus their application to cyber offences are either leading to conclusions against common sense[1082] or dependent on incidental elements of a crime,[1083] if they are not inapplicable at all. Recognising the fact that traditional criminal provisions are not adequate to apply, China promulgated computer specific provisions two decades ago, and have amended the provisions against cybercrime twice. When amending the cybercrime provisions, some scholars suggested to enact a separated and specific Act containing offences either targeting computer or facilitated by computer. They worried that cybercrime differs so much from traditional crimes that the CL cannot tackle cybercrime merely through inserting new provisions.[1084] The form of cyber-specific provisions is in fact a choice made in certain context and based on certain legal tradition. The US, England and Singapore all promulgated separate Act to stigmatise cyber wrongdoings in order to enhance the deterrence of the legislation, whereas China issues cybercrime provisions in order to make a comprehensive and all-inclusive CL. Thus, China can continue the current legislation and amend it when necessary, that is, when it fails to cover new forms of cyber wrongdoings.

(3) China should adopt a more systematic approach rather than relying on the concept of 'computer' as it currently does.

[1082] For the details see Chapter 5 Cybercrime Legislation in England.

[1083] For the details see Chapter 4 Cybercrime legislation in the US.

[1084] See e.g. Yu Zhigang, '网络思维的演变与网络犯罪的制裁思路' (The Evolution of Cyber Thinking and the Punishment of Cybercrime), *Peking University Law Journal*, 4(2014): 1045-1058.

The recommendation that China can keep cybercrime provisions in the Criminal Law does not mean China does not need to reconsider the approach it currently takes. As pointed out, the approach China takes, namely, focusing on the computer, leads to over-criminalisation and confusions among criminal provisions. Thus, China should adopt a more systematic approach in order to better regulate cybercrime domestically.

While recognising the approach China currently takes has some advantages, such as combating cybercrime to some extent and appling to most forms of cybercrimes, its disadvantages cannot be ignored. Firstly, the subtle boundary between extensive interpretation and analogical interpretation is threatened, or even broken, under this approach. As data, especially data stored on personal computers becomes more and more frequently targeted and damaged, the protection for the function of computer appears insufficient. For example, under the computer approach, one presumption must be satisfied before data can be protected. Namely, 'data' is somehow 'the function of computer'. In order to satisfy this presumption, if the data stored on a computer is damaged, the storage capability of computer must be understood as subsequently damaged, and thus the function of computer is damaged. However, the function of computer and the data are in essence different. This is because the former is protected for its capability to process the latter and the latter is protected for the information it delivers. Therefore, this presumption, or in another word, extension, of the function of computer to include the security of data raises issues such as how extensive the interpretation of cybercrime provisions can reach.

Secondly, the focus on computer may lead to a situation that the actor is incriminated merely because he used the computer to conduct his activity. The computer is protected on the reasoning that it has function and thus is valuable. This implies that computer is protected as property, as the same as other valuable devices like television and car. However, computer can also perform as the criminal tool. Thus, in a case where computer performs as the tool, the computer approach may result in the situation where the involvement of computer becomes the reason that lowering the threshold of criminal punishment. For instance, under Chinese definition the information network belongs to 'computer'. The Amendment (IX) inserts Article 287B to criminalise situations where an actor A knowingly provides **assistance** to the person B who is **using the information network** to commit crimes. Under this offence, if B has not used information network to commit a crime, A may not get criminal punishment, or may get a less severe punishment. To be clearer, if A knows B is going to use information network to commit online fraud, and A provides B Internet connection, A commits the

offence under Article 287B. In another situation, A knows B is going to rob a bank, and A provides B communication device, such as mobile phone, A may for a great possibility not be pursued criminal liability or may be pursued criminal liability as an accessory. It is thus clear that under this situation, it is the B's usage of the information network, rather than the severe consequence, that serves as the main reason for A's criminal punishment.

(4) China should adopt the computer and data approach. Distinguishing damage to the function of computer and damage to the security of data is the first step of this approach, and addressing them respectively through computer specific provisions is the second step.

This recommendation is the most important one of this research to China. The problems China is currently facing when dealing with cybercrime are to a large extent resulted from the computer approach it currently takes. Further, if it sticks to this approach, more issues will emerge, as the US experience shows. Thus, considering the advantages and disadvantages of three approaches, as well as China's current situation, this research proposes the computer and data approach. In addition, a mere protection of them is not enough. Instead, recognising computer and data are protected for different reasons and addressing them respectively is what this thesis suggests. This recommendation is proposed on the following reasons.

First of all, adopting the computer and data approach is better for participating in international affairs against cybercrime. 'The vast network of international telecommunications systems which facilitate cross-border cybercrime offending demands a common universal framework that is not just regionally centred or organizationally exclusive.'[1085] Ideally, this framework takes the form of an internationally binding legal instrument.[1086] The CoC is one of such a legal instrument, and it is by now the most widely adopted one. It is a successful convention not only because the international cooperation platforms it established. Moreover, it takes a systematic and consistent approach. Therefore, if China wants to join the international community and to cooperate against cybercrime, it is better to adopt the approach the CoC takes – the computer and data approach.

Secondly, compared with the current approach China adopts, the computer and data approach can contribute to protecting information, both state secret and privacy, which is currently

[1085] Cameron S. D. Brown, 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice', *International Journal of Cyber Criminology*, vol. 9 1(2015): 55-119, p. 91.

[1086] *Ibid*.

insufficient in China. The insufficiency of protection on data, or information, is one of the reasons that cybercrime cannot be effectively combated. For the first, data delivers personal information that can be used to commit crimes such as fraud; for the second, data also contains secrets, such as national defence information that can be used for terrorist attack. Thus, data needs to be confidential and remain unchanged. However, the computer approach cannot be sufficiently applied to offences against the confidentiality, integrity and availability of data. In contrast, the computer and data approach adopted in England and the CoE has proved its value on solving this issue without presenting more problems, compared with merely protecting the function of computer or merely protecting data. Thus, this approach can contribute to the protection of data in China as well.

Thirdly, the computer and data approach can contribute to restricting the infringement upon online freedom since it can to large extent avoid analogical interpretation. Merely protecting the function of computer or the security of data leads to an interpretation that *computer includes data*, or *data includes computer*. Such interpretation expands the scope of computer or data dramatically, and therefor becomes an analogy. Moreover, it delivers an impression that to tackle cybercrime, dramatic expansion of cyber-specific provisions is acceptable, even when such expansion amounts to analogical interpretation. It further delivers an idea that the principle of protecting foundamental rights from being infringed can give way to combating crime. Therefore, online freedom may be sacrificed under this consideration. If, as England and the CoE do, distinguish damage to the function of computer and damage to the security of data through legislation, such improper impression can be avoided to a large extent.

More importantly, through avoiding analogical interpretation, the computer and data approach can guide judges when adjudicating cybercrime cases. In the fast developing field of information technology, gaps between legislation and practice, between law in books and law in practice often exist. However, laws cannot be amended all the time. In this context, judges can take some responsibility on interpreting and applying the existing provisions, provided that necessary guidance is present. A consistent approach, coupled with clarified interest that protected under each provision, can serve as such necessary guidance. To be clearer, the computer and data approach in fact clarifies distinctions among relevant criminal provisions, and by doing so establishes a boundary between extensive interpretation and analogical interpretation. Thus, when adjudicating relevant cases, judges can firstly know how broad the provisions can reach, and secondly choose the most suitable provision dealing with the activity in question. By doing this, the confusions and overlaps among provisions, as

well as the uncertainties whether relevant provisions apply to new forms of cyber wrongdoings can be avoided to a large extent.

7.5 Final Remarks

This research hopes to contribute to a better regulation on cybercrime. As well known, the information network ties everyone in this world together. The crimes, and cybercrime in particular, have also 'benefited' from the information network. Some severe cybercrimes, such as cyber-terrorist attacks and child-pornography distribution, have been provided more opportunities by web-enabled computers. Seen in this light, initiating an in-depth discussion to find appropriate approaches to deter and combat cybercrime is an ultra-necessity. The US has long been a pioneer on this issue, and so have the UK, Singapore and the Council of Europe. China, although started to discuss this issue two decades' later, has also launched many projects on how to combat cybercrime. However, after decades of discussion and attempts, a final solution to cybercrime is still pending. Hardly any of the solutions seems optimistic considering the amount of cybercrime keeps rising. Given this, the author sincerely hopes the conclusions and recommendations proposed in this research could be, to a certain degree, while it is still unknown, helpful to improve the current situation.

Appendices

Appendix I Relevant Legal Provisions of the Chapter on China

Constitution (2004 amended)

Article 57

The National People's Congress of the People's Republic of China is the highest organ of state power. Its permanent body is the Standing Committee of the National People's Congress.

Article 89

The State Council exercises the following functions and powers:

to adopt administrative measures, enact administrative rules and regulations and issue decisions and orders in accordance with the Constitution and the law;

to submit proposals to the National People's Congress or its Standing Committee;

…

(13) …to alter or annul inappropriate orders, directives and regulations issued by the ministries or commissions;

(14) to alter or annul inappropriate decisions and orders issued by local organs of state administration at various levels;

…

Article 90

Ministers in charge of the ministries or commissions of the State Council are responsible for the work of their respective departments and they convene and preside over ministerial meetings or general and executive meetings of the commissions to discuss and decide on major issues in the work of their respective departments.

The ministries and commissions issue orders, directives and regulations within the jurisdiction of their respective departments and in accordance with the law and the administrative rules and regulations, decisions and orders issued by the State Council.

Article 127

The Supreme People's Court is the highest judicial organ.

The Supreme People's Court supervises the administration of justice by the people's courts at various local levels and by the special people's courts. People's courts at higher levels supervise the administration of justice by those at lower levels.

Organic Law of People’s Court (2006 amended)

Article 33

The Supreme People's Court gives interpretation on questions concerning specific application of laws and decrees in judicial proceeding.

Construction Law (2011 amended)

Article 65

…

An organization which contracts projects without a certificate of qualification shall be outlawed and imposed fine penalties, with all its illegal incomes confiscated.

An organization which has obtained a certificate of qualification through cheating shall be revoked the certificate and imposed fine penalties, and shall be prosecuted for criminal liabilities according to law for any crimes committed.

Criminal Law (2011 amended)

Article 6

This law is applicable to all who commit crimes within the territory of the PRC except as specially stipulated by law.

This law is also applicable to all who commit crimes aboard a ship or aircraft of the PRC.

When either the act or consequence of a crime takes place within PRC territory, a crime is deemed to have been committed within PRC territory.

Article 7

This law is applicable to PRC citizens who commit the crimes specified in this law outside the territory of the PRC; but those who commit the crimes, provided that this law stipulates a minimum sentence of less than a three-year fixed-term imprisonment for such crimes, may not be dealt with.

This law is applicable to PRC state personnel and military personnel who commit the crimes specified in this law outside PRC territory.

Article 8

This law may be applicable to foreigners, who outside PRC territory, commit crimes against the PRC state or against its citizens, provided that this law stipulates a minimum sentence of not less than a three-year fixed term of imprisonment for such crimes; but an exception is to be made if a crime is not punishable according the law of the place where it was committed.

Article 9

This law is applicable to the crimes specified in international treaties to which the PRC is a signatory state or with which it is a member and the PRC exercises criminal jurisdiction over such crimes within its treaty obligations.

Article 11

The problem of criminal responsibility of foreigners who enjoy diplomatic privileges and immunity is to be resolved through diplomatic channels.

Article 96

The phrase "violating state stipulations" in this law refers to violation of laws and decisions formulated by the National People's Congress or the National People's Congress Standing Committee; and administrative measures prescribed in administrative ordinance and regulations formulated by the State Council; as well as decisions and decrees the State Council promulgated.

Article 253A

Whoever sells or provides any citizen's personal information in violation of the relevant provisions of the state shall, if the circumstances are serious, be sentenced to imprisonment of not more than three years or criminal detention in addition to a fine or be sentenced to a fine only; or be sentenced to imprisonment of not less than three years but not more than seven years in addition to a fine if the circumstances are especially serious.

Whoever sells or provides to any other person any citizen's personal information obtained in the course of performing functions or providing services in violation of any relevant provisions of the state shall be given a heavier penalty in accordance with the provisions of the preceding paragraph.

Whoever illegally obtains any citizen's personal information by stealing or other methods shall be punished in accordance with the provisions of paragraph 1.

Where an entity commits any crime as provided for in the preceding three paragraphs, the entity shall be sentenced to a fine, and its directly responsible person in charge and other directly liable persons shall be punished according to the provisions of the applicable paragraph.

Article 264

Whoever steals a relatively large amount of public or private property, commits thefts many times, commits a burglary or carries a lethal weapon to steal or pick pockets shall be sentenced to imprisonment of not more than 3 years, criminal detention or control and/or a fine; if the amount involved is huge or there is any other serious circumstance, shall be sentenced to imprisonment of not less than 3 years but not more than 10 years and a fine; or if the amount involved is especially huge or there is any other especially serious circumstance, shall be sentenced to imprisonment of not less than 10 years or life imprisonment and a fine or forfeiture of property.

Article 274

Whoever extorts a relatively large amount of public or private property or extorts public or private property many times shall be sentenced to imprisonment of not more than 3 years, criminal detention or control and/or a fine; if the amount involved is huge or there is any other serious circumstance, shall be sentenced to imprisonment of not less than 3 years but not more than 10 year and a fine; or if the amount involved is especially huge or there is any other especially serious circumstance, shall be sentenced to imprisonment of not less than 10 years and a fine.

Article 285

Whoever violates state regulations and intrudes into computer systems with information concerning state affairs, construction of defence facilities, and sophisticated science and technology is be sentenced to not more than three years of fixed-term imprisonment or criminal detention.

Whoever, in violation of the state provisions, intrudes into a computer information system other than that prescribed in the preceding paragraph or uses other technical means to obtain the data stored, processed or transmitted in the said computer information system or exercise illegal control over the

said computer information system shall, if the circumstances are serious, be sentenced to fixed-term imprisonment not more than three years or criminal detention, and/or be fined; or if the circumstances are extremely serious, shall be sentenced to fixed-term imprisonment not less than three years but not more than seven years, and be fined.

Whoever provides special programs or tools specially used for intruding into or illegally controlling computer information systems, or whoever knows that any other person is committing the criminal act of intruding into or illegally controlling a computer information system and still provides programs or tools for such a person shall, if the circumstances are serious, be punished under the preceding paragraph.

Where an entity commits any crime as provided for in the preceding three paragraphs, the entity shall be sentenced to a fine, and its directly responsible person in charge and other directly liable persons shall be punished according to the provisions of the applicable paragraph.

Article 286

Whoever violates states regulations and deletes, alters, adds, and interferes in computer information systems, causing abnormal operations of the systems and grave consequences, is to be sentenced to not more than five years of fixed-term imprisonment or criminal detention; when the consequences are particularly serious, the sentence is to be not less than five years of fixed-term imprisonment.

Whoever violates state regulations and deletes, alters, or adds the data or application programs installed in or processed and transmitted by the computer systems, and causes grave consequences, is to be punished according to the preceding paragraph.

Whoever deliberately creates and propagates computer virus and other programs which sabotage the normal operation of the computer system and cause grave consequences is to be punished according to the first paragraph.

Where an entity commits any crime as provided for in the preceding three paragraphs, the entity shall be sentenced to a fine, and its directly responsible person in charge and other directly liable persons shall be punished according to the provisions of the applicable paragraph.

Article 286A

Any network service provider that fails to perform the information network security management obligation as prescribed in any law or administrative regulation and refuses to make corrections after being ordered by the regulatory authority to take correction measures shall be sentenced to imprisonment of not more than three years, criminal detention or surveillance in addition to a fine or be sentenced to a fine only under any of the following circumstances:

causing the spread of a large amount of illegal information;

causing the leakage of users' information, with serious consequences;

causing the loss of criminal case evidence, with serious circumstances;

any other serious circumstance.

Where an entity commits the crime as provided for in the preceding paragraph, a fine shall be imposed on it, and its directly responsible person in charge and other directly liable persons shall be punished in accordance with the provisions of the preceding paragraph.

Whoever commits any other crime while committing a crime as mentioned in the preceding two paragraphs shall be convicted and punished according to the provisions on the crime with the heavier penalty.

Article 287

Whoever uses a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing state secrets, or other crimes is to be convicted and punished according to relevant regulations of this law.

Article 287A

Whoever commits any of the following conducts by using the information network shall, if the circumstances are serious, be sentenced to imprisonment of not more than three years or criminal detention in addition to a fine or be sentenced to a fine only.

Establishing a website or a communication group mainly for committing fraud, teaching on how to commit a crime, producing or selling any prohibited or controlled article, or committing any other illegal or criminal activity.

Issuing any information on the production or sale of drugs, guns, obscene articles, or any other prohibited or controlled article or any other illegal or criminal conduct.

Issuing any information for committing fraud or any other illegal or criminal activity.

Where an entity commits any crime as provided for in the preceding paragraph, the entity shall be sentenced to a fine, and its directly responsible person in charge and other directly liable persons shall be punished in accordance with the provisions of paragraph 1.

Whoever commits any other crime while committing a crime as mentioned in the preceding two paragraphs shall be convicted and punished according to the provisions on the crime with the heavier penalty.

Article 287B

Whoever, while obviously aware that any other person is committing a crime by using an information network, provides Internet access, server custody, network storage, communication transmission or any other technical support, or provides advertising, payment settlement or any other assistance for the crime shall, if the circumstances are serious, be sentenced to imprisonment of not more than three years or criminal detention in addition to a fine or be sentenced to a fine only.

Where an entity commits any crime as provided for in the preceding paragraph, the entity shall be sentenced to a fine, and its directly responsible person in charge and other directly liable persons shall be punished in accordance with the provisions of paragraph 1.

Whoever commits any other crime while committing a crime as mentioned in the preceding two paragraphs shall be convicted and punished according to the provisions on the crime with the heavier penalty.

Legislation Law (2015 amended)

Article 7

The National People's Congress and its Standing Committee shall exercise the legislative power of the State.

The National People's Congress shall develop and amend the basic laws on criminal matters, civil matters, and state authorities, among others.

The Standing Committee of the National People's Congress shall develop and amend laws other than those developed by the National People's Congress; and when the National People's Congress is not in session, partially supplement and amend laws developed by the National People's Congress, provided that the basic principles in such laws are not violated.

Article 65

The State Council shall develop administrative regulations in accordance with the Constitution and laws.

The following matters may be governed by administrative regulations:

(1) matters requiring the development of administrative regulations to implement the provisions of laws;

(2) matters within the administrative functions and powers of the State Council as set out in Article 89 of the Constitution;

…

Article 72

The people's congress and its standing committee of a province, autonomous region, or municipality directly under the Central Government may, according to the specific circumstances and actual needs of the administrative region, develop local regulations, provided that such regulations do not contravene the Constitution, laws, and administrative regulations.

…

Article 73

The following matters may be governed by local regulations:

(1) matters requiring the development of specific provisions according to the actual circumstances of the administrative region in order to implement the provisions of laws or administrative regulations;

(2) matters as local affairs that require the development of local regulations;

…

Article 104

The interpretations on specific application of law in trial or procuratorial work as developed by the Supreme People's Court or the Supreme People's Procuratorate shall primarily involve the specific clauses of laws and conform to the objectives, principles, and original meaning of legislation. Under any of the circumstances as set out in paragraph 2, Article 45 of this Law, a request for legal interpretation or a proposal for developing or amending a relevant law shall be submitted to the Standing Committee of the National People's Congress.

…

Judicial interpretations

Interim Provisions of the SPC and the SPP on the Management of International Networking of Computer Information Networks 1997 revised

Article 9

Supply units of international exit and entry channels, the competent departments or the competent units of internetworking units should, in pursuance of the relevant provisions of law and the state, be responsible for the work of security protection of international exit and entry channels and the subordinate internetworking.

Provisions of the SPC on Citation of Such Normative Legal Documents as Laws and Regulations in the Judgements 2009

Article 3

A criminal judgement shall cite laws, legal interpretations or judicial interpretations. Article 4 of these Provisions shall apply to the citation of normative legal documents in judgements of civil suits collateral to criminal proceedings.

Provisions of the SPC Concerning Work on Guiding Cases 2010

Article 7

Where the Case Guidance Office finds it necessary to conduct further research on a potential guiding case, it may consult relevant state authorities, departments, and social organizations, members of the Case Guidance Expert Committee, experts and scholars.

Interpretation of the SPC and the SPP of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems 2011

Article 1

If any person who illegally obtains the computer information system data or controls the computer information system falls under any of the following circumstances, it shall be deemed that "the circumstances involved are serious" as specified in Paragraph 2 of Article 285 of the Criminal Law:

1. Where more ten pieces of identity authentication information on network-based financial services such as payment and settlement, securities trading and futures trading are obtained;

2. Where more than five hundred pieces of identity authentication information other than those in Item 1 of this Article are obtained;

3. Where more than twenty computer information systems are illegally controlled;

4. Where the illegal income is more than 5,000 yuan or an economic loss of more 10,000 yuan is incurred; or

5. Any other situation in which the circumstances involved are serious.

If any person who commits any of the acts specified in the preceding paragraph fall under any of the following circumstances, it shall be deemed as that "the circumstances involved are extremely serious" as specified in Paragraph 2 of Article 285 of the Criminal Law:

1. Where the number or amount is more than fivefold of that specified in Items 1 to 4 in the preceding paragraph; or

2. Any other situation in which the circumstances involved are extremely serious.

If any person who knows that another person illegally controls the computer information system uses the control over the computer information system, he or she shall be convicted and punished in accordance with the preceding two paragraphs.

Article 11

The 'computer information system' or 'computer system' as mentioned in this Interpretation refers to a system having the function of automatic processing of data, including computers, network equipment, communications equipment, automatic control equipment, etc.

The 'identity verification information' as mentioned in this Interpretation refers to the data used for identifying the operating authorisation for a user of a computer information system, including account number, key, password, digital certificate, etc.

Interpretations of the Supreme People's Court on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks 2012

Article 15

A civil dispute case involving infringement of the right of dissemination on information networks shall be under the jurisdiction of the people's court at the place of infringement or the place of domicile of the defendant. The place of infringement includes the place where the network server, computer terminal or any other equipment used for committing the alleged infringement is located. Where it is difficult to determine both the place of infringement and the place of domicile of the defendant or both of them are located outside China, the place where the computer terminal or any other equipment on which the plaintiff discovers the infringing content is located may be deemed the place of infringement.

Interpretation of the SPC and the SPP on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Theft 2013

Article 1

Whoever steals public or private property of 1,000 yuan to 3,000 yuan and more, 30,000 yuan to 100,000 yuan and more, or 300,000 yuan to 500,000 yuan and more shall be deemed to respectively fall within the scope of 'relatively large amount', 'large amount' and 'extraordinarily large amount' as prescribed in Article 264 of the Criminal Law.

The higher people's courts and the people's procuratorates of all provinces, autonomous regions and municipalities directly under the Central Government may, in light of the economic development status of their respective regions, and in consideration of the social security situation, determine, within the scope of the amounts specified in the preceding paragraph, specific amount standards for their respective regions, and report them to the Supreme People's Court and the Supreme People's Procuratorate for approval.

Where a theft is omitted in a public transportation vehicle which is operated across different regions, and the theft location cannot be verified, the issue of whether the amount of theft reaches 'relatively large amount', 'large amount', or 'extraordinarily large amount' shall be determined in accordance with the relevant amount standards determined by the higher people's court and the people's procuratorate of the province, autonomous region or municipality directly under the Central Government where the case is accepted.

Where the theft of drugs or any other contraband should be punished according to the crime of theft, sentencing shall be rendered in light of the seriousness of circumstances.

Governmental regulations and Administrative rules

Regulations of the People's Republic of China for Safety Protection of Computer Information Systems 1994

Article 2

A computer information system referred to in these Regulations means a man-machine system composed of a computer and its related and complementary sets of equipment and facilities (including network) which carry out collection, processing, storage, transmission, retrieval and other operations of information in accordance with specific application aims and rules.

Article 12

Anyone who transports, carries or posts media of computer information into or out of this country shall make truthful declaration to the Customs.

Article 13

An organization using the computer information system shall establish and improve a system of safety management, and shall be responsible for the safety protection of its own computer information.

Regulations on the Administration of Business Sites of Internet Access Services 2002

Article 19

An operating entity shall use technical measures for its management, establish the system of in-house patrol, and if finding out any act listed in Articles 14, 15, 18 of the present Regulations or other illegal acts by the Internet users, stop such acts immediately and report to the departments of cultural administration and public security.

Measures for Security Protection in the Administration of the International Networking of Computer Information Networks (2011 revised)

Article 4

No unit or individual shall use the international networking to endanger state security, divulge state secrets, nor shall it/he/she infringe on national, social and collective interests and the legitimate rights and interests of citizens, nor shall it/he/she engage in illegal criminal activities.

Appendix II Relevant Legal Provisions of the Chapter on the Council of Europe

The Convention on Cybercrime

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Title 1 – 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.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result 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 intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

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.

Title 2 – 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.

Title 3 – 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 conduct;

c realistic 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.

Title 4 – Offences related to infringements of copyright and related right

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.

The Explanatory Report of the Convention on Cybercrime

Article 10

In addition, the CDPC took into account the Report, prepared – at its request – by Professor H.W.K. Kaspersen, which concluded that '… it should be looked to another legal instrument with more engagement than a Recommendation, such as a Convention. Such a Convention should not only deal with criminal substantive law matters, but also with criminal procedural questions as well as with international criminal law procedures and agreements.' A similar conclusion emerged already from the Report attached to Recommendation N° R (89) 9 concerning substantive law and from Recommendation N° R (95) 13 concerning problems of procedural law connected with information technology.

Article 18

Section 1 of Chapter II (substantive law issues) covers both criminalisation provisions and other connected provisions in the area of computer- or computer-related crime: it first defines 9 offences grouped in 4 different categories, then deals with ancillary liability and sanctions. The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights.

Introduction to the definitions at Article 1

Article 22

It was understood by the drafters that under this Convention Parties would not be obliged to copy verbatim into their domestic laws the four concepts defined in Article 1, provided that these laws cover such concepts in a manner consistent with the principles of the Convention and offer an equivalent framework for its implementation.

Article 23 - Article 1 (a) – Computer system of the Convention on Cybercrime

A computer system under the Convention is a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities. It may stand alone or be connected in a network with other similar devices "Automatic" means without direct human intervention, "processing of data" means that data in the computer system is operated by executing a computer program. A "computer program" is a set of instructions that can be executed by the computer to achieve the intended result. A computer can run different programs. A computer system usually consists of different devices, to be distinguished as the processor or central processing unit, and peripherals. A "peripheral" is a device that performs certain specific functions in interaction with the processing unit, such as a printer, video screen, CD reader/writer or other storage device.

Article 25 - Article 1 (b) – Computer data of the Convention on Cybercrime

The definition of computer data builds upon the ISO-definition of data. This definition contains the terms "suitable for processing". This means that data is put in such a form that it can be directly processed by the computer system. In order to make clear that data in this Convention has to be understood as data in electronic or other directly processable form, the notion 'computer data' is introduced. Computer data that is automatically processed may be the target of one of the criminal

offences defined in this Convention as well as the object of the application of one of the investigative measures defined by this Convention.

Article 26 - Article 1 (c) – Service provider of the Convention on Cybercrime

The term "service provider" encompasses a broad category of persons that play a particular role with regard to communication or processing of data on computer systems (cf. also comments on Section 2). Under (i) of the definition, it is made clear that both public and private entities which provide users the ability to communicate with one another are covered. Therefore, it is irrelevant whether the users form a closed group or whether the provider offers its services to the public, whether free of charge or for a fee. The closed group can be e.g. the employees of a private enterprise to whom the service is offered by a corporate network.

Article 29 - Article 1 (d) – Traffic data of the Convention on Cybercrime

In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive.

Article 30

The definition lists exhaustively the categories of traffic data that are treated by a specific regime in this Convention: the origin of a communication, its destination, route, time (GMT), date, size, duration and type of underlying service. Not all of these categories will always be technically available, capable of being produced by a service provider, or necessary for a particular criminal investigation. The "origin" refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services. The "destination" refers to a comparable indication of a communications facility to which communications are transmitted. The term "type of underlying service" refers to the type of service that is being used within the network, e.g., file transfer, electronic mail, or instant messaging.

Section 1 – Substantive criminal law of the Convention on Cybercrime

Article 38

A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression ‘without right’ derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party’s government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised. Specific

examples of such exceptions from criminalisation are provided in relation to specific offences in the corresponding text of the Explanatory Memorandum below. It is left to the Parties to determine how such exemptions are implemented within their domestic legal systems (under criminal law or otherwise).

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems of the Convention on Cybercrime

Article 44- Illegal access (Article 2) of the Convention on Cybercrime

"Illegal access" covers the basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data. The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner. The mere unauthorised intrusion, i.e. "hacking", "cracking" or "computer trespass" should in principle be illegal in itself. It may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction. Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.

Article 49

Many national legislations already contain provisions on "hacking" offences, but the scope and constituent elements vary considerably. The broad approach of criminalisation in the first sentence of Article 2 is not undisputed. Opposition stems from situations where no dangers were created by the mere intrusion or where even acts of hacking have led to the detection of loopholes and weaknesses of the security of systems. This has led in a range of countries to a narrower approach requiring additional qualifying circumstances which is also the approach adopted by Recommendation N° (89) 9 and the proposal of the OECD Working Party in 1985.

Article 50

Parties can take the wide approach and criminalise mere hacking in accordance with the first sentence of Article 2. Alternatively, Parties can attach any or all of the qualifying elements listed in the second sentence: infringing security measures, special intent to obtain computer data, other dishonest intent that justifies criminal culpability, or the requirement that the offence is committed in relation to a computer system that is connected remotely to another computer system. The last option allows Parties to exclude the situation where a person physically accesses a stand-alone computer without any use of another computer system. They may restrict the offence to illegal access to networked computer systems (including public networks provided by telecommunication services and private networks, such as Intranets or Extranets).

Article 51 - Illegal interception (Article 3) of the Convention on Cybercrime

This provision aims to protect the right of privacy of data communication. The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights. The offence established under Article 3 applies this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer.

Article 53

Interception by ‘technical means’ relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalisation.

Article 54

The offence applies to ‘non-public’ transmissions of computer data. The term ‘non-public’ qualifies the nature of the transmission (communication) process and not the nature of the data transmitted. The data communicated may be publicly available information, but the parties wish to communicate confidentially. Or data may be kept secret for commercial purposes until the service is paid, as in Pay-TV. Therefore, the term ‘non-public’ does not per se exclude communications via public networks. Communications of employees, whether or not for business purposes, which constitute "non-public transmissions of computer data" are also protected against interception without right under Article 3 (see e.g. ECHR Judgement in Halford v. UK case, 25 June 1997, 20605/92).

Article 58

For criminal liability to attach, the illegal interception must be committed "intentionally", and "without right". The act is justified, for example, if the intercepting person has the right to do so, if he acts on the instructions or by authorisation of the participants of the transmission (including authorised testing or protection activities agreed to by the participants), or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities. It was also understood that the use of common commercial practices, such as employing ‘cookies’, is not intended to be criminalised as such, as not being an interception "without right". With respect to non-public communications of employees protected under Article 3 (see above paragraph 54), domestic law may provide a ground for legitimate interception of such communications. Under Article 3, interception in such circumstances would be considered as undertaken "with right".

Article 64 - Data interference (Article 4) of the Convention on Cybercrime

Paragraph 2 allows Parties to enter a reservation concerning the offence in that they may require that the conduct result in serious harm. The interpretation of what constitutes such serious harm is left to domestic legislation, but Parties should notify the Secretary General of the Council of Europe of their interpretation if use is made of this reservation possibility.

Article 65 - System interference (Article 5) of the Convention on Cybercrime

This is referred to in Recommendation No. (89) 9 as computer sabotage. The provision aims at criminalising the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data. The protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly. The text is formulated in a neutral way so that all kinds of functions can be protected by it.

Article 67

The hindering must furthermore be "serious" in order to give rise to criminal sanction. Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered "serious." For example, a Party may require a minimum amount of damage to be caused in order for

the hindering to be considered serious. The drafters considered as "serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g., by means of programs that generate "denial of service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system).

Article 69

The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ("spamming"). In the opinion of the drafters, such conduct should only be criminalised where the communication is intentionally and seriously hindered. Nevertheless, Parties may have a different approach to hindrance under their law, e.g. by making particular acts of interference administrative offences or otherwise subject to sanction. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law.

Article 71 - Misuse of devices (Article 6) of the Convention on Cybercrime

This provision establishes as a separate and independent criminal offence the intentional commission of specific illegal acts regarding certain devices or access data to be misused for the purpose of committing the above-described offences against the confidentiality, the integrity and availability of computer systems or data. As the commission of these offences often requires the possession of means of access ("hacker tools") or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of a kind of black market in their production and distribution. To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5. In this respect the provision builds upon recent developments inside the Council of Europe (European Convention on the legal protection of services based on, or consisting of, conditional access – ETS N° 178) and the European Union (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access) and relevant provisions in some countries. A similar approach has already been taken in the 1929 Geneva Convention on currency counterfeiting.

Article 73

The drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The alternative to include all devices even if they are legally produced and distributed was also rejected. Only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment, an approach which in the area of money counterfeiting also has not been adopted. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices.

Article 77

Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system is not covered by the provision. This concept is already contained in the expression

'without right'. For example, test-devices ('cracking-devices') and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be 'with right'.

Title 2 – Computer-related offences of the Convention on Cybercrime

Article 79

Articles 7 – 10 relate to ordinary crimes that are frequently committed through the use of a computer system. Most States already have criminalised these ordinary crimes, and their existing laws may or may not be sufficiently broad to extend to situations involving computer networks (for example, existing child pornography laws of some States may not extend to electronic images). Therefore, in the course of implementing these articles, States must examine their existing laws to determine whether they apply to situations in which computer systems or networks are involved. If existing offences already cover such conduct, there is no requirement to amend existing offences or enact new ones.

Article 81 - Computer-related Forgery (Article 7) of the Convention on Cybercrime

The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception. The protected legal interest is the security and reliability of electronic data which may have consequences for legal relations.

Article 82

It should be noted that 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 minimum to the issuer of the data, regardless of the correctness or veracity of the contents of the data. Parties may go further and include under the term "authentic" the genuineness of the data.

Article 86 - Computer-related fraud (Article 8) of the Convention on Cybercrime

With the arrival of the technological revolution the opportunities for committing economic crimes such as fraud, including credit card fraud, have multiplied. Assets represented or administered in computer systems (electronic funds, deposit money) have become the target of manipulations like traditional forms of property. These crimes consist mainly of input manipulations, where incorrect data is fed into the computer, or by programme manipulations and other interferences with the course of data processing. The aim of this article is to criminalise any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property.

Article 87

To ensure that all possible relevant manipulations are covered, the constituent elements of 'input', 'alteration', 'deletion' or 'suppression' in Article 8(a) are supplemented by the general act of 'interference with the functioning of a computer programme or system' in Article 8(b). The elements of 'input, alteration, deletion or suppression' have the same meaning as in the previous articles. Article

8(b) covers acts such as hardware manipulations, acts suppressing printouts and acts affecting recording or flow of data, or the sequence in which programs are run.

Article 90

The offence has to be committed "intentionally". The general intent element refers to the computer manipulation or interference causing loss of property to another. The offence also requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another. Thus, for example, commercial practices with respect to market competition that may cause an economic detriment to a person and benefit to another, but are not carried out with fraudulent or dishonest intent, are not meant to be included in the offence established by this article. For example, the use of information gathering programs to comparison shop on the Internet ("bots"), even if not authorised by a site visited by the "bot" is not intended to be criminalised.

Title 3 – Content-related offences of the Convention on Cybercrime

Article 91 - Offences related to child pornography (Article 9) of the Convention on Cybercrime

Article 9 on child pornography seeks to strengthen protective measures for children, including their protection against sexual exploitation, by modernising criminal law provisions to more effectively circumscribe the use of computer systems in the commission of sexual offences against children.

Article 93

This provision criminalises various aspects of the electronic production, possession and distribution of child pornography. Most States already criminalise the traditional production and physical distribution of child pornography, but with the ever-increasing use of the Internet as the primary instrument for trading such material, it was strongly felt that specific provisions in an international legal instrument were essential to combat this new form of sexual exploitation and endangerment of children. It is widely believed that such material and on-line practices, such as the exchange of ideas, fantasies and advice among paedophiles, play a role in supporting, encouraging or facilitating sexual offences against children.

Article 95

Paragraph 1(b) criminalises the ‘offering’ of child pornography through a computer system. ‘Offering’ is intended to cover soliciting others to obtain child pornography. It implies that the person offering the material can actually provide it. ‘Making available’ is intended to cover the placing of child pornography on line for the use of others e.g. by means of creating child pornography sites. This paragraph also intends to cover the creation or compilation of hyperlinks to child pornography sites in order to facilitate access to child pornography.

Article 98

The possession of child pornography in a computer system or on a data carrier, such as a diskette or CD-Rom, is criminalised in paragraph 1(e). The possession of child pornography stimulates demand for such material. An effective way to curtail the production of child pornography is to attach criminal consequences to the conduct of each participant in the chain from production to possession.

Article 100

A ‘sexually explicit conduct’ covers at least real or simulated: a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between minors, or between an adult and a

minor, of the same or opposite sex; b) bestiality; c) masturbation; d) sadistic or masochistic abuse in a sexual context; or e) lascivious exhibition of the genitals or the pubic area of a minor. It is not relevant whether the conduct depicted is real or simulated.

Article 101

The three types of material defined in paragraph 2 for the purposes of committing the offences contained in paragraph 1 cover depictions of sexual abuse of a real child (2a), pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct (2b), and finally images, which, although 'realistic', do not in fact involve a real child engaged in sexually explicit conduct (2c). This latter scenario includes pictures which are altered, such as morphed images of natural persons, or even generated entirely by the computer.

Title 4 – Offences related to infringements of copyright and related rights

Article 107 - Offences related to infringements of copyright and related rights (Article 10) of the Convention on Cybercrime

Infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet, which cause concern both to copyright holders and those who work professionally with computer networks. The reproduction and dissemination on the Internet of protected works, without the approval of the copyright holder, are extremely frequent. Such protected works include literary, photographic, musical, audio-visual and other works. The ease with which unauthorised copies may be made due to digital technology and the scale of reproduction and dissemination in the context of electronic networks made it necessary to include provisions on criminal law sanctions and enhance international co-operation in this field.

Article 113

Copyright and related rights offences must be committed "wilfully" for criminal liability to apply. In contrast to all the other substantive law provisions of this Convention, the term "wilfully" is used instead of "intentionally" in both paragraphs 1 and 2, as this is the term employed in the TRIPS Agreement (Article 61), governing the obligation to criminalise copyright violations.

Section 3 – Jurisdiction

Article 233 - Jurisdiction (Article 22) of the Convention on Cybercrime

Paragraph 1 littera a is based upon the principle of territoriality. Each Party is required to punish the commission of crimes established in this Convention that are committed in its territory. For example, a Party would assert territorial jurisdiction if both the person attacking a computer system and the victim system are located within its territory, and where the computer system attacked is within its territory, even if the attacker is not.

Article 236

Paragraph 1, littera d is based upon the principle of nationality. The nationality theory is most frequently applied by States applying the civil law tradition. It provides that nationals of a State are obliged to comply with the domestic law even when they are outside its territory. Under littera d, if a national commits an offence abroad, the Party is obliged to have the ability to prosecute it if the conduct is also an offence under the law of the State in which it was committed or the conduct has taken place outside the territorial jurisdiction of any State.

Article 239

In the case of crimes committed by use of computer systems, there will be occasions in which more than one Party has jurisdiction over some or all of the participants in the crime. For example, many virus attacks, frauds and copyright violations committed through use of the Internet target victims located in many States. In order to avoid duplication of effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials of the States concerned, or to otherwise facilitate the efficiency or fairness of the proceedings, the affected Parties are to consult in order to determine the proper venue for prosecution. In some cases, it will be most effective for the States concerned to choose a single venue for prosecution; in others, it may be best for one State to prosecute some participants, while one or more other States pursue others. Either result is permitted under this paragraph. Finally, the obligation to consult is not absolute, but is to take place "where appropriate." Thus, for example, if one of the Parties knows that consultation is not necessary (e.g., it has received confirmation that the other Party is not planning to take action), or if a Party is of the view that consultation may impair its investigation or proceeding, it may delay or decline consultation.

Appendix III Relevant Legal Provisions of the Chapter on the United States

17 U.S.C. § 506 Criminal Offences

17 U.S.C. § 506 (a)(1)

Any person who wilfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed—

(A) for purposes of commercial advantage or private financial gain;

(B) by the reproduction or distribution, including by electronic means, during any 180–day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000; or

(C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution.

18 U.S.C. § 1028 Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information

18 U.S.C. § 1028 (a)

Whoever, in a circumstance described in subsection (c) of this section—

(1) knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document;

(2) knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority;

(3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents;

(4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States;

(5) knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used;

(6) knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States or a sponsoring entity of an event designated as a special event of national significance which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority;

(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or

(8) knowingly traffics in false or actual authentication features for use in false identification documents, document-making implements, or means of identification; shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 1028 (d)(1)

The term 'authentication feature' means any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified.

18 U.S.C. § 1028 (d)(2)

The term 'document-making implement' means any implement, impression, template, computer file, computer disc, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making implement.

18 U.S.C. § 1028 (d)(3)

The term 'identification document' means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a sponsoring entity of an event designated as a special event of national significance, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals.

18 U.S.C. § 1028 (d)(4)

The term 'false identification document' means a document of a type intended or commonly accepted for the purposes of identification of individuals that—

(A) is not issued by or under the authority of a governmental entity or was issued under the authority of a governmental entity but was subsequently altered for purposes of deceit; and

(B) appears to be issued by or under the authority of the United States Government, a State, a political subdivision of a State, a sponsoring entity of an event designated by the President as a special event of national significance, a foreign government, a political subdivision of a foreign government, or an international governmental or quasi-governmental organization.

18 U.S.C. § 1028 (d)(7)

The term 'means of identification' means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—

(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device (as defined in section 1029 (e)).

18 U.S.C. § 1029 Fraud and Related Activity In Connection With Access Devices

18 U.S.C. § 1029 (a)

Whoever—

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorised access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorised access devices;

(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

(6) without the authorisation of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of—

(A) offering an access device; or

(B) selling information regarding or an application to obtain an access device;

(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorised use of telecommunications services;

(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorisation; or

(10) without the authorisation of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device; shall, if the offence affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

18 U.S.C. § 1029 (e)(1)

The term ‘access device’ means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

18 U.S.C. § 1029(e)(5)

The term ‘traffic’ means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of.

18 U.S.C. § 1030 Fraud and Related Activity in Connection with Computers

18 U.S.C. § 1030 (a)

Whoever—

(1) having knowingly accessed a computer without authorisation or exceeding authorised access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorised disclosure for reasons of national defence or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation wilfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or wilfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorisation or exceeds authorised access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorisation to access any non-public computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorisation, or exceeds authorised access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorisation, to a protected computer;

(B) intentionally accesses a protected computer without authorisation, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorisation, and as a result of such conduct, causes damage and loss.

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorisation, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorisation or in excess of authorisation or to impair the confidentiality of information obtained from a protected computer without authorisation or by exceeding authorised access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030 (b)

Whoever conspires to commit or attempts to commit an offence under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030 (c)

The punishment for an offence under subsection (a) or (b) of this section is—

(1)

(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offence under subsection (a)(1) of this section which does not occur after a conviction for another offence under this section, or an attempt to commit an offence punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offence under subsection (a)(1) of this section which occurs after a conviction for another offence under this section, or an attempt to commit an offence punishable under this subparagraph;

(2)

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offence under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offence under this section, or an attempt to commit an offence punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offence under subsection (a)(2), or an attempt to commit an offence punishable under this subparagraph, if—

(i) the offence was committed for purposes of commercial advantage or private financial gain;

(ii) the offence was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offence under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offence under this section, or an attempt to commit an offence punishable under this subparagraph;

(3)

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offence under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offence under this section, or an attempt to commit an offence punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offence under subsection (a)(4), or (a)(7) of this section which occurs after a conviction for another offence under this section, or an attempt to commit an offence punishable under this subparagraph;

(4)

(A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—

(i) an offence under subsection (a)(5)(B), which does not occur after a conviction for another offence under this section, if the offence caused (or, in the case of an attempted offence, would, if completed, have caused)—

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defence, or national security; or

(VI) damage affecting 10 or more protected computers during any 1-year period; or

(ii) an attempt to commit an offence punishable under this subparagraph;

(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i) an offence under subsection (a)(5)(A), which does not occur after a conviction for another offence under this section, if the offence caused (or, in the case of an attempted offence, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii) an attempt to commit an offence punishable under this subparagraph;

(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of—

(i) an offence or an attempt to commit an offence under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offence under this section; or

(ii) an attempt to commit an offence punishable under this subparagraph;

(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i) an offence or an attempt to commit an offence under subsection (a)(5)(C) that occurs after a conviction for another offence under this section; or

(ii) an attempt to commit an offence punishable under this subparagraph;

(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G) a fine under this title, imprisonment for not more than 1 year, or both, for—

(i) any other offence under subsection (a)(5); or

(ii) an attempt to commit an offence punishable under this subparagraph.

18 U.S.C. § 1030 (d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offences under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offences under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorised disclosure for reasons of national defence or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014 (y)), except for offences affecting the duties of the United States Secret Service pursuant to section 3056 (a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

18 U.S.C. § 1030 (e)

As used in this section—

(1) the term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(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 or 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;

(3) the term 'State' includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term 'financial institution' means—

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term 'financial record' means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term ‘exceeds authorised access’ means to access a computer with authorisation and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term ‘department of the United States’ means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8) the term ‘damage’ means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term ‘government entity’ includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term ‘conviction’ shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorised access, or exceeding authorised access, to a computer;

(11) the term ‘loss’ means any reasonable cost to any victim, including the cost of responding to an offence, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offence, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term ‘person’ means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

18 U.S.C. § 1343 Fraud by Wire, Radio, or Television

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretences, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation occurs in relation to, or involving any benefit authorised, transported, transmitted, transferred, disbursed, or paid in connection with, a presidentially declared major disaster or emergency (as those terms are defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122)), or affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

18 U.S.C. § 2251 Sexual Exploitation of Children

18 U.S.C. § 2251 (a)

Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

18 U.S.C. § 2251 A(a)

Any parent, legal guardian, or other person having custody or control of a minor who sells or otherwise transfers custody or control of such minor, or offers to sell or otherwise transfer custody of such minor either—

(1) with knowledge that, as a consequence of the sale or transfer, the minor will be portrayed in a visual depiction engaging in, or assisting another person to engage in, sexually explicit conduct; or

(2) with intent to promote either—

(A) the engaging in of sexually explicit conduct by such minor for the purpose of producing any visual depiction of such conduct; or

(B) the rendering of assistance by the minor to any other person to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct;

shall be punished by imprisonment for not less than 30 years or for life and by a fine under this title, if any of the circumstances described in subsection (c) of this section exist.

18 U.S.C. § 2252 Certain Activities Relating to Material Involving the Sexual Exploitation of Minors

18 U.S.C. § 2252 (a)

Any person who—

(1) knowingly transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mails, any visual depiction, if—

(A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(B) such visual depiction is of such conduct;

(2) knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through themails, if—

(A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(B) such visual depiction is of such conduct;

(3) either—

(A) in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the Government of the United States, or in the Indian country as defined in section 1151 of this title, knowingly sells or possesses with intent to sell any visual depiction; or

(B) knowingly sells or possesses with intent to sell any visual depiction that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce, or has been shipped or transported in or affecting interstate or foreign commerce, or which was produced using

materials which have been mailed or so shipped or transported using any means or facility of interstate or foreign commerce, including by computer, if—

(i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(ii) such visual depiction is of such conduct; or

(4) either—

(A) in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the Government of the United States, or in the Indian country as defined in section 1151 of this title, knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction; or

(B) knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if—

(i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(ii) such visual depiction is of such conduct;

shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 2252 A(a)

Any person who—

(1) knowingly mails, or transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography;

(2) knowingly receives or distributes—

(A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or

(B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

(3) knowingly—

(A) reproduces any child pornography for distribution through themails, or using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer; or

(B) advertises, promotes, presents, distributes, or solicits through themails, or using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains—

(i) an obscene visual depiction of a minor engaging in sexually explicit conduct; or

(ii) a visual depiction of an actual minor engaging in sexually explicit conduct;

(4) either—

(A) in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the United States Government, or in the Indian country (as defined in section 1151), knowingly sells or possesses with the intent to sell any child pornography; or

(B) knowingly sells or possesses with the intent to sell any child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

(5) either—

(A) in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the United States Government, or in the Indian country (as defined in section 1151), knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography; or

(B) knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

(6) knowingly distributes, offers, sends, or provides to a minor any visual depiction, including any photograph, film, video, picture, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, where such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct—

(A) that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer;

(B) that was produced using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer; or

(C) which distribution, offer, sending, or provision is accomplished using themails or any means or facility of interstate or foreign commerce, for purposes of inducing or persuading a minor to participate in any activity that is illegal; or

(7) knowingly produces with intent to distribute, or distributes, by any means, including a computer, in or affecting interstate or foreign commerce, child pornography that is an adapted or modified depiction of an identifiable minor

shall be punished as provided in subsection (b).

18 U.S.C. § 2256 Definitions for Chapter

18 U.S.C. § 2256 (8)

'Child pornography' means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where—

(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

(C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

18 U.S.C. § 2260 Production of Sexually Explicit Depictions of A Minor for Importation into the United States

18 U.S.C. § 2260 (a) Use of Minor

A person who, outside the United States, employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor with the intent that the minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, intending that the visual depiction will be imported or transmitted into the United States or into waters within 12 miles of the coast of the United States, shall be punished as provided in subsection (c).

18 U.S.C. § 2260 (b) Use of Visual Depiction

A person who, outside the United States, knowingly receives, transports, ships, distributes, sells, or possesses with intent to transport, ship, sell, or distribute any visual depiction of a minor engaging in sexually explicit conduct (if the production of the visual depiction involved the use of a minor engaging in sexually explicit conduct), intending that the visual depiction will be imported into the United States or into waters within a distance of 12 miles of the coast of the United States, shall be punished as provided in subsection (c).

18 U.S.C. § 2510 Definitions

18 U.S.C. § 2510 (1)

'Wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

18 U.S.C. § 2510 (2)

'Oral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication.

18 U.S.C. § 2510 (8)

'Contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.

18 U.S.C. § 2510 (12)

'Electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

18 U.S.C. § 2511 Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited

18 U.S.C. § 2511 (1)(a)

Any person who—

(a) intentionally intercepts, endeavours to intercept, or procures any other person to intercept or endeavour to intercept, any wire, oral, or electronic communication;

…

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

18 U.S.C. § 2701 Unlawful Access to Stored Communications

18 U.S.C. § 2701 (a)

Whoever—

(1) intentionally accesses without authorisation a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorisation to access that facility; and thereby obtains, alters, or prevents authorised access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 3121 General Prohibition on Pen Register and Trap and Trace Device Use; Exception

18 U.S.C. § 3121 (a)

No person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978.

18 U.S.C. § 3127 Definitions for Chapter

18 U.S.C. § 3127 (3)

The term ‘pen register’ means a device or process which records or decodes dialling, routing, addressing, or signalling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

18 U.S.C. § 3127 (4)

The term ‘trap and trace device’ means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialling, routing, addressing, and signalling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

Appendix IV Relevant Legal Provisions of the Chapter on England

Theft Act 1968

Section 13 Abstracting of electricity

A person who dishonestly uses without due authority, or dishonestly causes to be wasted or diverted, any electricity shall on conviction on indictment be liable to imprisonment for a term not exceeding five years.

Criminal Damage Act 1971

Section 1(1)

A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence.

Protection of Children Act 1978

Section 1(1)

(1) It is an offence for a person—

(a) to take, or permit to be taken or to make, any indecent photographor pseudo-photographof a child; or

(b) to distribute or show such indecent photographs or pseudo-photographs; or

(c) to have in his possession such indecent photographs or pseudo-photographs, with a view to their being distributed or shown by himself or others; or

(d) to publish or cause to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photographs or pseudo-photographs, or intends to do so.

Section 7 Interpretation

(1) The following subsections apply for the interpretation of this Act.

(2) References to an indecent photograph include an indecent film, a copy of an indecent photograph or film, and an indecent photograph comprised in a film.

(3) Photographs (including those comprised in a film) shall, if they show children and are indecent, be treated for all purposes of this Act as indecent photographs of children and so as respects pseudo-photographs.

(4) References to a photograph include—

(a) the negative as well as the positive version; and

(b) data stored on a computer disc or by other electronic means which is capable of conversion into a photograph.

(5) 'Film' includes any form of video-recording.

(6) 'Child', subject to subsection (8), means a person under the age of 16.

(7) 'Pseudo-photograph' means an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph.

(8) If the impression conveyed by a pseudo-photograph is that the person shown is a child, the pseudo-photograph shall be treated for all purposes of this Act as showing a child and so shall a pseudo-photograph where the predominant impression conveyed is that the person shown is a child notwithstanding that some of the physical characteristics shown are those of an adult.

(9) References to an indecent pseudo-photograph include—

(a) a copy of an indecent pseudo-photograph; and

(b) data stored on a computer disc or by other electronic means which is capable of conversion into a pseudo-photograph.

Forgery and Counterfeiting Act 1981

Section 1

A person is guilty of forgery if he makes a false instrument, with the intention that he or another shall use it to induce somebody to accept it as genuine, and by reason of so accepting it to do or not to do some act to his own or any other person's prejudice.

Section 8(1)

Subject to subsection (2) below, in this Part of this Act 'instrument' means—

(a) any document, whether of a formal or informal character;

(b) any stamp issued or sold by a postal operator;

(c) any Inland Revenue stamp; and

(d) any disc, tape, sound track or other device on or in which information is recorded or stored by mechanical, electronic or other means.

Copyright, Designs and Patents Act 1988

Section 104 Presumptions relevant to literary, dramatic, musical and artistic works

(1) The following presumptions apply in proceedings brought by virtue of this Chapter with respect to a literary, dramatic, musical or artistic work.

(2) Where a name purporting to be that of the author appeared on copies of the work as published or on the work when it was made, the person whose name appeared shall be presumed, until the contrary is proved—

(a) to be the author of the work;

(b) to have made it in circumstances not falling within section 11(2), 163, 165 or 168 (works produced in course of employment, Crown copyright, Parliamentary copyright or copyright of certain international organisations).(3)In the case of a work alleged to be a work of joint authorship, subsection (2) applies in relation to each person alleged to be one of the authors.

(4) Where no name purporting to be that of the author appeared as mentioned in subsection (2) but—

(a) the work qualifies for copyright protection by virtue of section 155 (qualification by reference to country of first publication), and

(b) a name purporting to be that of the publisher appeared on copies of the work as first published, the person whose name appeared shall be presumed, until the contrary is proved, to have been the owner of the copyright at the time of publication.

(5) If the author of the work is dead or the identity of the author cannot be ascertained by reasonable inquiry, it shall be presumed, in the absence of evidence to the contrary—

(a) that the work is an original work, and

(b) that the plaintiff's allegations as to what was the first publication of the work and as to the country of first publication are correct.

Section 107 (1), (2) and (2A)

(1) A person commits an offence who, without the licence of the copyright owner—

(a) makes for sale or hire, or

(b) imports into the United Kingdom otherwise than for his private and domestic use, or

(c) possesses in the course of a business with a view to committing any act infringing the copyright, or

(d) in the course of a business —

(i) sells or lets for hire, or

(ii) offers or exposes for sale or hire, or

(iii) exhibits in public, or

(iv) distributes, or

(e) distributes otherwise than in the course of a business to such an extent as to affect prejudicially the owner of the copyright, an article which is, and which he knows or has reason to believe is, an infringing copy of a copyright work.

(2) A person commits an offence who—

(a) makes an article specifically designed or adapted for making copies of a particular copyright work, or

(b) has such an article in his possession, knowing or having reason to believe that it is to be used to make infringing copies for sale or hire or for use in the course of a business.

(2A) A person who infringes copyright in a work by communicating the work to the public—

(a) in the course of a business, or

(b) otherwise than in the course of a business to such an extent as to affect prejudicially the owner of the copyright, commits an offence if he knows or has reason to believe that, by doing so, he is infringing copyright in that work.

Computer Misuse Act 1990

Section 1 Unauthorised access to computer material

(1) A person will be found guilty if

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer or to enable any such access to be secured;

(b) the access he intends to secure or to enable to be secured is unauthorised; and he knows at the time when he causes the computer to perform the function that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

Section 2 Unauthorised access with intent to commit or facilitate commission of further offences

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ('the unauthorised access offence') with intent—

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person); and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences—

(a) for which the sentence is fixed by law; or

(b) for which a person who has attained the age of twenty-one years (eighteen in relation to England and Wales) and has no previous convictions may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates' Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

Section 3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

(1) A person is guilty of an offence if—

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if 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;

(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) to (c) above to be done.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) 'act' includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

(6) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both.

Section 3A Making, supplying or obtaining articles for use in offence under section 1 or 3

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(3) A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.

(4) In this section 'article' includes any program or data held in electronic form.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

Section 4 Territorial scope of offences under sections 1 to 3

(1) Except as provided below in this section, it is immaterial for the purposes of any offence under section 1 or 3 above—

(a) whether any act or other event proof of which is required for conviction of the offence occurred in the home country concerned; or

(b) whether the accused was in the home country concerned at the time of any such act or event.

(2) Subject to subsection (3) below, in the case of such an offence at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the offence to be committed.

(3) There is no need for any such link to exist for the commission of an offence under section 1 above to be established in proof of an allegation to that effect in proceedings for an offence under section 2 above.

(4) Subject to section 8 below, where—

(a) any such link does in fact exist in the case of an offence under section 1 above; and

(b) commission of that offence is alleged in proceedings for an offence under section 2 above; section 2 above shall apply as if anything the accused intended to do or facilitate in any place outside the home country concerned which would be an offence to which section 2 applies if it took place in the home country concerned were the offence in question.

(5) This section is without prejudice to any jurisdiction exercisable by a court in Scotland apart from this section.

(6) References in this Act to the home country concerned are references—

(a) in the application of this Act to England and Wales, to England and Wales;

(b) in the application of this Act to Scotland, to Scotland; and

(c) in the application of this Act to Northern Ireland, to Northern Ireland.

Section 9(a)

In any proceedings brought in England and Wales in respect of any offence to which this section applies it is immaterial to guilt whether or not the accused was a British citizen at the time of any act, omission or other event proof of which is required for conviction of the offence.

Section 17(5)

Access of any kind by any person to any program or data held in a computer is unauthorised if—

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled but this subsection is subject to section 10.

Section 17(6)

References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

Data Protection Act 1998

Section 55(1)

A person must not knowingly or recklessly, without the consent of the data controller—

(a) obtain or disclose personal data or the information contained in personal data, or

(b) procure the disclosure to another person of the information contained in personal data.

Criminal Justice and Court Service Act 2000

Section 41(3)

In section 160 of the Criminal Justice Act 1988 (summary offence of possession of indecent photograph of child)—

(a)after subsection (2) there is inserted—

'(2A) A person shall be liable on conviction on indictment of an offence under this section to imprisonment for a term not exceeding five years or a fine, or both.',

(b)for the sidenote there is substituted 'Possession of indecent photograph of child'.

Regulation of Investigatory Powers Act 2000

Section 1 Unlawful interception

(1) It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of—

(a) a public postal service; or

(b) a public telecommunication system.

(2) It shall be an offence for a person—

(a) intentionally and without lawful authority, and

(b) otherwise than in circumstances in which his conduct is excluded by subsection (6) from criminal liability under this subsection, to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system.

(3) Any interception of a communication which is carried out at any place in the United Kingdom by, or with the express or implied consent of, a person having the right to control the operation or the use of a private telecommunication system shall be actionable at the suit or instance of the sender or recipient, or intended recipient, of the communication if it is without lawful authority and is either—

(a) an interception of that communication in the course of its transmission by means of that private system; or

(b) an interception of that communication in the course of its transmission, by means of a public telecommunication system, to or from apparatus comprised in that private telecommunication system.

(4) Where the United Kingdom is a party to an international agreement which—

(a) relates to the provision of mutual assistance in connection with, or in the form of, the interception of communications,

(b) requires the issue of a warrant, order or equivalent instrument in cases in which assistance is given, and

(c) is designated for the purposes of this subsection by an order made by the Secretary of State,

it shall be the duty of the Secretary of State to secure that no request for assistance in accordance with the agreement is made on behalf of a person in the United Kingdom to the competent authorities of a country or territory outside the United Kingdom except with lawful authority.

(5) Conduct has lawful authority for the purposes of this section if, and only if—

(a) it is authorised by or under section 3 or 4;

(b) it takes place in accordance with a warrant under section 5 ('an interception warrant'); or

(c) it is in exercise, in relation to any stored communication, of any statutory power that is exercised (apart from this section) for the purpose of obtaining information or of taking possession of any document or other property; and conduct (whether or not prohibited by this section) which has lawful authority for the purposes of this section by virtue of paragraph (a) or (b) shall also be taken to be lawful for all other purposes.

(6) The circumstances in which a person makes an interception of a communication in the course of its transmission by means of a private telecommunication system are such that his conduct is excluded from criminal liability under subsection (2) if—

(a) he is a person with a right to control the operation or the use of the system; or

(b) he has the express or implied consent of such a person to make the interception.

(7) A person who is guilty of an offence under subsection (1) or (2) shall be liable—

(a) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both;

(b) on summary conviction, to a fine not exceeding the statutory maximum.

(8) No proceedings for any offence which is an offence by virtue of this section shall be instituted—

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland.

Section 2 (1), (2) and (5)

(1) In this Act—

'private telecommunication system' means any telecommunication system which, without itself being a public telecommunication system, is a system in relation to which the following conditions are satisfied—

(a) it is attached, directly or indirectly and whether or not for the purposes of the communication in question, to a public telecommunication system; and

(b) there is apparatus comprised in the system which is both located in the United Kingdom and used (with or without other apparatus) for making the attachment to the public telecommunication system; 'public telecommunications service' means any telecommunications service which is offered or provided to, or to a substantial section of, the public in any one or more parts of the United Kingdom;

(2) For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he—

(a) so modifies or interferes with the system, or its operation,

(b) so monitors transmissions made by means of the system, or

(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.

(5) References in this Act to the interception of a communication in the course of its transmission by means of a postal service or telecommunication system do not include references to—

(a) any conduct that takes place in relation only to so much of the communication as consists in any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted; or

(b) any such conduct, in connection with conduct falling within paragraph (a), as gives a person who is neither the sender nor the intended recipient only so much access to a communication as is necessary for the purpose of identifying traffic data so comprised or attached.

Identity Cards Act 2006

Section 25(1) and (3)

(1) It is an offence for a person with the requisite intention to have in his possession or under his control—

(a) an identity document that is false and that he knows or believes to be

false;

(b) an identity document that was improperly obtained and that he knows or believes to have been improperly obtained; or

(c) an identity document that relates to someone else.

(3) It is an offence for a person with the requisite intention to make, or to have in his possession or under his control—

(a) any apparatus which, to his knowledge, is or has been specially designed or adapted for the making of false identity documents; or

(b) any article or material which, to his knowledge, is or has been specially designed or adapted to be used in the making of false identity documents.

Section 26(1) Identity documents for the purposes of s. 25

(1) In section 25 'identity document' means any document that is, or purports to be—

(a) an ID card;

(b) a designated document;

(c) an immigration document;

(d) a United Kingdom passport (within the meaning of the Immigration Act 1971 (c. 77));

(e) a passport issued by or on behalf of the authorities of a country or territory outside the United Kingdom or by or on behalf of an international organisation;

(f) a document that can be used (in some or all circumstances) instead of a passport;

(g) a UK driving licence; or

(h) a driving licence issued by or on behalf of the authorities of a country or territory outside the United Kingdom.

Section 27(2)

For the purposes of this section a person is required to keep information confidential if it is information that is or has become available to him by reason of his holding an office or employment the duties of which relate, in whole or in part, to—

(a) the establishment or maintenance of the Register;

(b) the issue, manufacture, modification, cancellation or surrender of ID cards; or

(c) the carrying out of the Commissioner's functions.

Fraud Act 2006

Section 2 Fraud by false representation

(1) A person is in breach of this section if he—

(a) dishonestly makes a false representation, and

(b) intends, by making the representation—

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss.

(2) A representation is false if—

(a) it is untrue or misleading, and

(b) the person making it knows that it is, or might be, untrue or misleading.

(3) 'Representation' means any representation as to fact or law, including a representation as to the state of mind of—

(a) the person making the representation, or

(b) any other person.

(4) A representation may be express or implied.

(5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

Appendix V Relevant Legal Provisions of the Chapter on Singapore

Computer Misuse Act 1993

Long Title

An Act to make provision for securing computer material against unauthorised access or modification and for matters related thereto.

Section 2(1) Interpretation

In this Act, unless the context otherwise requires —

'computer' means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility;

'computer service' includes computer time, data processing and the storage or retrieval of data;

'data' means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

'electronic, acoustic, mechanical or other device' means any device or apparatus that is used or is capable of being used to intercept any function of a computer;

'function' includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer;

'intercept', in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof;

'program or computer program' means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

Section 4 Unauthorised access with intent to commit or facilitate commission of further offences

(1) Any person who causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

(2) This section shall apply to offences involving property, fraud, dishonesty or which causes bodily harm punishable on conviction with imprisonment for a term of 2 years or more.

(3) For the purposes of this section, it is immaterial whether the offence to which this section applies is to be committed at the same time when the unauthorised access is secured or on any future occasion.

Section 5 Unauthorised modification of computer material

(1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $2,000 or to imprisonment for a term not exceeding 2 years or to both.

(2) If any damage caused by an offence under this section exceeds $10,000, a person convicted of the offence shall be liable to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at —

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

Section 8 Territorial scope of offences under this Act

(1) Subject to subsection (2), the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore; and where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore.

(2) For the purposes of subsection (1), this Act shall apply if, for the offence in question —

(a) the accused was in Singapore at the material time; or

(b) the computer, program or data was in Singapore at the material time.

Section 14 Powers of police officer to investigate and require assistance

In connection with the exercise of his powers of investigations under the Criminal Procedure Code (Cap. 68), a police officer —

(a) shall be entitled at any time to have access to, and inspect and check the operation of, any computer and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offence under this Act; and

(b) may require —

(i) the person by whom or on whose behalf the police officer has reasonable cause to suspect the computer is or has been so used; or

(ii) any person having charge of, or otherwise concerned with the operation of, the computer, apparatus or material, to provide him with such reasonable assistance as he may require for the purposes of paragraph (a).

Evidence (Amendment) Act 1996

Amendment of section 3

'Computer' means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include —

(a) an automated typewriter or typesetter;

(b) a portable hand held calculator;

(c) a device similar to those referred to in paragraphs (a) and (b) which is non-programmable or which does contain any data storage facility;

(d) such other device as the Minister may by notification prescribe.

Computer Misuse (Amendment) Act 1998

Amendment of section 2

Section 2(1) of the Computer Misuse Act (referred to in this Act as the principal Act) is amended —

(a) by deleting the words 'but does not include an automated typewriter or typesetter, a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility;' at the end of the definition of 'computer' and substituting the following words:

but does not include —

(a) an automated typewriter or typesetter;

(b) a portable hand held calculator;

(c) a similar device which is non-programmable or which does not contain any data storage facility; or

(d) such other device as the Minister may, by notification in the Gazette, prescribe; and

(b) by inserting, immediately after the definition of 'computer service', the following definition:

'damage' means, except for the purposes of section 10, any impairment to a computer or the integrity or availability of data, a program or system, or information, that —

(a) causes loss aggregating at least $10,000 in value, or such other amount as the Minister may, by notification in the Gazette, prescribe except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account;

(b) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of one or more persons;

(c) causes or threatens physical injury or death to any person; or

(d) threatens public health or public safety;'.

New sections 6A, 6B and 6C

6A. Unauthorised obstruction of use of computer

(1) Any person who knowingly and without authority or lawful excuse —

(a) interferes with, or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

6B. Unauthorised disclosure of access code

(1) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if he did so —

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) knowing that it is likely to cause wrongful loss to any person.

(2) Any person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

6C. Enhanced punishment for offences involving protected computers

(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 6A, the person convicted of such an offence shall, in lieu of the punishment prescribed in those sections, be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 20 years or to both.

(2) For the purposes of subsection (1), a computer shall be treated as a 'protected computer' if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for —

(a) the security, defence or international relations of Singapore;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.

(3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer or program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer or program or data attracts an enhanced penalty under this section.'

Computer Misuse (Amendment) Act 2003

New section 15A

15A. Preventing or countering threats to national security, etc.

(1) Where the Minister is satisfied that it is necessary for the purposes of preventing or countering any threat to the national security, essential services, defence or foreign relations of Singapore, the Minister may, by a certificate under his hand, authorise any person or organisation specified in the certificate to take such measures as may be necessary to prevent or counter any threat to a computer or computer service or any class of computers or computer services.

(2) The measures referred to in subsection (1) may include, without limitation, the exercise by the authorised person or organisation of the powers referred to in section 15.

(3) Where an offence is disclosed in the course of or pursuant to the exercise of any power under this section —

(a) no information for that offence shall be admitted in evidence in any civil or criminal proceedings; and

(b) no witness in any civil or criminal proceedings shall be obliged —

(i) to disclose the name, address or other particulars of any informer who has given information with respect to that offence; or

(ii) to answer any question if the answer would lead, or would tend to lead, to the discovery of the name, address or other particulars of the informer.

(4) If any book, document, data or computer output which is admitted in evidence or liable to inspection in any civil or criminal proceedings contain any entry in which any informer is named or described or which may lead to his discovery, the court shall cause those entries to be concealed from view or to be obliterated so far as may be necessary to protect the informer from discovery.

(5) In subsection (1), 'essential services' means —

(a) services directly related to communications infrastructure, banking and finance, public utilities, public transportation or public key infrastructure; and

(b) emergency services such as police, civil defence or medical services.'.

Computer Misuse Act (Chapter 50A) 2013 amended

Section 2(1) and (2) Interpretation

(1) In this Act, unless the context otherwise requires —

'computer' means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include —

(a) an automated typewriter or typesetter;

(b) a portable hand-held calculator;

(c)a similar device which is non-programmable or which does not contain any data storage facility; or

(d) such other device as the Minister may, by notification in the Gazette, prescribe;

'computer output' or 'output' means a statement or representation (whether in written, printed, pictorial, graphical or other form) purporting to be a statement or representation of fact —

(a) produced by a computer; or

(b) accurately translated from a statement or representation so produced;

'computer service' includes computer time, data processing and the storage or retrieval of data;

'damage' means, except for the purposes of section 13, any impairment to a computer or the integrity or availability of data, a program or system, or information, that —

(a) causes loss aggregating at least $10,000 in value, or such other amount as the Minister may, by notification in the Gazette, prescribe except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account;

(b) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of one or more persons;

(c) causes or threatens physical injury or death to any person; or

(d) threatens public health or public safety;

'data' means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

'electro-magnetic, acoustic, mechanical or other device' means any device or apparatus that is used or is capable of being used to intercept any function of a computer;

'function' includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer;

'intercept', in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof;

'program or computer program' means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

(2) For the purposes of this Act, a person secures access to any program or data held in a computer if by causing a computer to perform any function he —

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner), and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

Section 3 Unauthorised access to computer material

(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at —

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer'

[ECMA 1990, s. 1]

Section 4 Access with intent to commit or facilitate commission of offence

(1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence.

(2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

(3) Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

(4) For the purposes of this section, it is immaterial whether —

(a) the access referred to in subsection (1) is authorised or unauthorised;

(b) the offence to which this section applies is committed at the same time when the access is secured or at any other time.

[UK CMA 1990, s. 2]

Section 5 Unauthorised modification of computer material

(1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at —

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

[ECMA 1990, s. 3]

Section 6 Unauthorised use or interception of computer service

(1) Subject to subsection (2), any person who knowingly —

(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at —

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

[Canada CLAA 1985, s. 301.2 (1)]

Section 7 Unauthorised obstruction of use of computer

(1) Any person who, knowingly and without authority or lawful excuse —

(a) interferes with, or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

Section 8 Unauthorised disclosure of access code

(1) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if he did so —

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) knowing that it is likely to cause wrongful loss to any person.

(2) Any person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

Section 9 Enhanced punishment for offences involving protected computers

(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such an offence shall, in lieu of the punishment prescribed in those sections, be liable to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 20 years or to both.

(2) For the purposes of subsection (1), a computer shall be treated as a 'protected computer' if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for —

(a) the security, defence or international relations of Singapore;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.

(3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, program or data attracts an enhanced penalty under this section.

Section 10 Abetments and attempts punishable as offences

(1) Any person who abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.

(2) For an offence to be committed under this section, it is immaterial where the act in question took place.

Section 11 Territorial scope of offences under this Act

(1) Subject to subsection (2), the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore.

(2) Where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore.

(3) For the purposes of this section, this Act shall apply if, for the offence in question —

(a) the accused was in Singapore at the material time; or

(b) the computer, program or data was in Singapore at the material time.

[ECMA 1990, ss. 4 and 5]

Section 12A Composition of offences

(1) The Commissioner of Police or any person authorised by him may, in his discretion, compound any offence under this Act which is prescribed as a compoundable offence by collecting from a person reasonably suspected of having committed the offence a sum not exceeding $3,000.

(2) The Minister may make regulations to prescribe the offences which may be compounded.

Legislative Source Key

Unless otherwise stated, the abbreviations used in the references to other Acts and statutory provisions are references to the following Acts and statutory provisions. The references are provided for convenience of users and are not part of the Act:

UK CMA 1990: United Kingdom, Computer Misuse Act 1990 (c. 18)

Canada CLAA 1985:Canada, Criminal Law Amendment Act 1985 (c. 19)

S Aust. EA 1929: South Australia, Evidence Act 1929

Internal Security Act (Chapter 143) 1987

Section 8

(1) If the President is satisfied with respect to any person that, with a view to preventing that person from acting in any manner prejudicial to the security of Singapore or any part thereof or to the maintenance of public order or essential services therein, it is necessary to do so, the Minister shall make an order —

(a) directing that such person be detained for any period not exceeding two years; or

(b) for all or any of the following purposes:

(i) for imposing upon that person such restrictions as may be specified in the order in respect of his activities and the places of his residence and employment;

(ii) for prohibiting him from being out of doors between such hours as may be specified in the order, except under the authority of a written permit granted by such authority or person as may be so specified;

(iii) for requiring him to notify his movements in such manner at such times and to such authority or person as may be specified in the order;

(iv) for prohibiting him from addressing public meetings or from holding office in, or taking part in the activities of or acting as adviser to any organisation or association, or from taking part in any political activities;

(v) for prohibiting him from travelling beyond the limits of Singapore or any part thereof specified in the order except in accordance with permission given to him by such authority or person as may be specified in such order,

and any order made under paragraph (b) shall be for such period, not exceeding two years, as may be specified therein, and may by such order be required to be supported by a bond.

(2) The President may direct that the period of any order made under subsection (1) be extended for a further period or periods not exceeding two years at a time.

(3) For the purposes of subsection (1), 'essential services' means any service, business, trade, undertaking, manufacture or calling included in the Third Schedule.

(4) Every person detained in pursuance of an order made under subsection (1)(a) or of a direction given under subsection (2) shall be detained in such place as the Minister may direct (hereinafter referred to as a place of detention) and in accordance with instructions issued by the Minister and any rules made under subsection (5).

(5) The Minister may by rules provide for the maintenance and management of any place of detention and for the discipline of persons detained therein.

Films Act (Chapter 107) 1998

Section 21 Penalty for possession, exhibition or distribution of uncensored films

(1) Any person who —

(a) has in his possession;

(b) exhibits or distributes; or

(c) reproduces,

any film without a valid certificate, approving the exhibition of the film, shall be guilty of an offence and shall be liable on conviction —

in respect of an offence under paragraph (a), to a fine of not less than $100 for each such film that he had in his possession (but not to exceed in the aggregate $20,000); and

in respect of an offence under paragraph (b) or (c), to a fine of not less than $500 for each such film he had exhibited, distributed or reproduced, as the case may be (but not to exceed in the aggregate $40,000) or to imprisonment for a term not exceeding 6 months or to both.

(2) Any Censor and any Deputy or Assistant Censor and any Inspector of Films may at all reasonable times enter any place in which any film is kept or is being or is about to be exhibited and may examine the film, and if on such examination he has reasonable grounds for believing that an offence under this section has been or is about to be committed in respect of the film he may seize the film and any equipment used in the commission of the offence.

(3) Any film and equipment seized under subsection (2) in respect of which any person has been convicted under this section shall be forfeited and shall be destroyed or otherwise disposed of in such manner as the Minister may direct.

(4) For the purposes of this section if any film is altered in any way after it has been approved for exhibition under this Act, the film shall be deemed not to have been so approved.

Undesirable Publication Act (Chapter 338) 1998

Section 2 Interpretation

'Publication' means any of the following other than a film:

(a) any book, magazine or periodical, whether in manuscript or final form;

(b) any sound recording;

(c) any picture or drawing, whether made by computer-graphics or otherwise howsoever;

(d) any photograph, photographic negative, photographic plate or photographic slide; or

(e) any paper, model, sculpture, tape, disc, article or thing —

(i) that has printed or impressed upon it any word, statement, sign or representation; or

(ii) on which is recorded or stored for immediate or future retrieval any information that, by the use of any computer or other electronic device, is capable of being reproduced or shown as any picture, photograph, word, statement, sign or representation, and includes a copy of any publication.

Section 3 Meaning of obscene

For the purposes of this Act, a publication is obscene if its effect or (where the publication comprises 2 or more distinct parts or items) the effect of any one of its parts or items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

Section 4 Meaning of objectionable

(1) For the purposes of this Act, a publication is objectionable if, in the opinion of any controller, it or (where the publication comprises 2 or more distinct parts or items) any one of its parts or items describes, depicts, expresses or otherwise deals with —

(a) matters such as sex, horror, crime, cruelty, violence or the consumption of drugs or other intoxicating substances in such a manner that the availability of the publication is likely to be injurious to the public good; or

(b) matters of race or religion in such a manner that the availability of the publication is likely to cause feelings of enmity, hatred, ill-will or hostility between different racial or religious groups.

(2) In determining for the purposes of this Act whether or not any publication is objectionable, the following matters shall be considered:

(a) the extent and degree to which, and the manner in which, the publication —

(i) describes, depicts or otherwise deals with acts of torture, the infliction of serious physical harm, sexual conduct or violence or coercion in association with sexual conduct;

(ii) exploits the nudity of persons or children or both;

(iii) promotes or encourages criminal acts or acts of terrorism;

(iv) represents, directly or indirectly, that members of any particular community or group are inherently inferior to other members of the public or of any other community or group;

(b) the impact of the medium in which the publication is presented;

(c) the character of the publication, including any merit, value or importance that the publication has in relation to literary, artistic, social, cultural, educational, scientific or other matters;

(d) the standards of morality, decency and propriety that are generally accepted by reasonable members of the community; and

(e) the persons, classes of persons or age groups of the persons to whom the publication is intended or is likely to be made available.

(3) The question whether or not a publication is objectionable is a matter for the expert judgement of any person authorised or required by or pursuant to this Act to determine it, and evidence as to or proof of any of the matters or particulars that the person is required to consider in determining that question is not essential to its determination except that if such evidence or proof of such matters or particulars is available, that person shall take that evidence or proof into consideration.

(4) The Chief Controller shall keep and maintain a Register of Objectionable Publications containing all publications which any controller determines to be objectionable.

Section 11 Offences involving obscene publications

Any person who —

(a) makes or reproduces, or makes or reproduces for the purposes of sale, supply, exhibition or distribution to any other person;

(b) imports or has in his possession for the purposes of sale, supply, exhibition or distribution to any other person; or

(c) sells, offers for sale, supplies, offers to supply, exhibits or distributes to any other person,

any obscene publication (not being a prohibited publication) knowing or having reasonable cause to believe the publication to be obscene shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 2 years or to both.

Section 12 Offences involving objectionable publications

Any person who —

(a) makes or reproduces, or makes or reproduces for the purposes of sale, supply, exhibition or distribution to any other person;

(b) imports or has in his possession for the purposes of sale, supply, exhibition or distribution to any other person; or

(c) sells, offers for sale, supplies, offers to supply, exhibits or distributes to any other person,

any objectionable publication (not being a prohibited publication) knowing or having reasonable cause to believe the publication to be objectionable shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 12 months or to both.

Copyright Act (Chapter 63) 2006

Section 136(3A)

Where, at any time when copyright subsists in a work —

(a) a person does any act that constitutes an infringement of the copyright in a work other than an act referred to in subsection (1), (2), (3) or (6);

(b) the infringement of the copyright in the work by the person is wilful; and

(c) either or both of the following apply:

(i) the extent of the infringement is significant;

(ii) the person does the act to obtain a commercial advantage,

the person shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 6 months or to both and, in the case of a second or subsequent offence, to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 3 years or to both.

Penal Code (Chapter 224) 2008

Section 22 Movable property

The words ‘movable property’ are intended to include corporeal property of every description, except land and things attached to the earth, or permanently fastened to anything which is attached to the earth.

Section 79 Act done by a person justified, or by mistake of fact believing himself justified by law

Nothing is an offence which is done by any person who is justified by law, or who by reason of a mistake of fact and not by reason of a mistake of law in good faith believes himself to be justified by law, in doing it.

Section 379 Punishment for theft

Whoever commits theft shall be punished with imprisonment for a term which may extend to 3 years, or with fine, or with both.

Section 415 Cheating

Whoever, by deceiving any person, whether or not such deception was the sole or main inducement, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit to do if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to any person in body, mind, reputation or property, is said to 'cheat'.

Explanation 1.—A dishonest concealment of facts is a deception within the meaning of this section.

Explanation 2.—Mere breach of contract is not of itself proof of an original fraudulent intent.

Explanation 3.—Whoever makes a representation through any agent is to be treated as having made the representation himself.

Section 425 Mischief

Whoever, with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or any person, causes the destruction of any property, or any such change in any property, or in the situation thereof, as destroys or diminishes its value or utility, or affects it injuriously, commits 'mischief".

Explanation 1.—It is not essential to the offence of mischief that the offender should intend to cause loss or damage to the owner of the property injured or destroyed. It is sufficient if he intends to cause, or knows that he is likely to cause, wrongful loss or damage to any person by injuring any property, whether it belongs to that person or not.

Explanation 2.—Mischief may be committed by an act affecting property belonging to the person who commits the act, or to that person and others jointly.

Personal Data Protection Act 2012

Section 2 Interpretation

'Evaluative purpose' means

(a) for the purpose of determining the suitability, eligibility or qualifications of the individual to whom the data relates —

(i) for employment or for appointment to office;

(ii) for promotion in employment or office or for continuance in employment or office;

(iii) for removal from employment or office;

(iv) for admission to an education institution;

(v) for the awarding of contracts, awards, bursaries, scholarships, honours or other similar benefits;

(vi) for selection for an athletic or artistic purpose; or

(vii) for grant of financial or social assistance, or the delivery of appropriate health services, under any scheme administered by a public agency;

(b) for the purpose of determining whether any contract, award, bursary, scholarship, honour or other similar benefit should be continued, modified or cancelled;

(c) for the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property; or

(d) for such other similar purposes as may be prescribed by the Minister.

Judicial Proceedings (Regulation of Publication) Act (Chapter 149) 2013

Section 2 Restriction on publication of reports

(1) It shall not be lawful to print or publish, or cause or procure to be printed or published —

(a) in relation to any judicial proceedings any indecent matter or indecent medical, surgical or physiological details being matter or details the publication of which would be calculated to injure public morals; or

(b) in relation to any judicial proceedings for divorce, dissolution of marriage, nullity of marriage, judicial separation or restitution of conjugal rights, any particulars other than the following:

(i) the names, addresses and occupations of the parties and witnesses;

(ii) a concise statement of the charges, the defences and counter charges in support of which evidence has been given;

(iii) submissions on any point of law arising in the course of the proceedings and the decision of the court on the submissions; and

(iv) the decision of the court and any observations made by the court in giving that decision.

(2) Nothing in subsection (1)(b) shall be held to permit the publication of anything contrary to subsection (1)(a).

Section 3 Penalty

Any person who acts in contravention of section 2 shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $1,000 or to imprisonment for a term not exceeding one year or to both:

Provided that no person, other than the proprietor, editor, printer or publisher, shall be liable to be convicted under this Act.

Canadian Criminal Code 1985 Rev. Ed.

Section 342.1(1) unauthorised use of computer (inserted by the Canada Criminal Amendment Act 1985, section 302.1(1))

Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service;

(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;

(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system; or

(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c).

International Covenant on Civil and Political Rights

Article 14

1. All persons shall be equal before the courts and tribunals. In the determination of any criminal charge against him, or of his rights and obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law. The press and the public may be excluded from all or part of a trial for reasons of morals, public order (order public) or national security in a democratic society, or when the interest of the private lives of the parties so requires, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice; but any judgement rendered in a criminal case or in a suit at law shall be made public except where the interest of juvenile persons otherwise requires or the proceedings concern matrimonial disputes or the guardianship of children.

2. Everyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law.

3. In the determination of any criminal charge against him, everyone shall be entitled to the following minimum guarantees, in full equality:

(a) To be informed promptly and in detail in a language which he understands of the nature and cause of the charge against him;

(b) To have adequate time and facilities for the preparation of his defence and to communicate with counsel of his own choosing;

(c) To be tried without undue delay;

(d) To be tried in his presence, and to defend himself in person or through legal assistance of his own choosing; to be informed, if he does not have legal assistance, of this right; and to have legal assistance assigned to him, in any case where the interests of justice so require, and without payment by him in any such case if he does not have sufficient means to pay for it;

(e) To examine, or have examined, the witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

(f) To have the free assistance of an interpreter if he cannot understand or speak the language used in court;

(g) Not to be compelled to testify against himself or to confess guilt.

4. In the case of juvenile persons, the procedure shall be such as will take account of their age and the desirability of promoting their rehabilitation.

5. Everyone convicted of a crime shall have the right to his conviction and sentence being reviewed by a higher tribunal according to law.

6. When a person has by a final decision been convicted of a criminal offence and when subsequently his conviction has been reversed or he has been pardoned on the ground that a new or newly discovered fact shows conclusively that there has been a miscarriage of justice, the person who has suffered punishment as a result of such conviction shall be compensated according to law, unless it is proved that the non-disclosure of the unknown fact in time is wholly or partly attributable to him.

7. No one shall be liable to be tried or punished again for an offence for which he has already been finally convicted or acquitted in accordance with the law and penal procedure of each country.

Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attack.

Bibliography

Adams, Jo-Ann M. 'Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet', *Computer and High Technology Law*, 12 (1996): 403-434.

Aldesco, Albert I. 'The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime', *Loyola of Los Angeles Entertainment Law Review*, vol. 23(2002): 81-123.

Ashworth, Andrew & Horder, Jeremy. *Principles of Criminal Law* (7th edition), Oxford: Oxford University Press, 2013.

Brenner, Susan W. 'Cybercrime Metrics: Old Wine, New Bottle?' *Virginia Journal of Law and Technology*, vol. 9 13(2004): 1-53.

Brenner, Susan W. 'U.S. Cybercrime Law: Defining Offences', *Information Systems Frontiers*, 6(2004): 115-132.

Carr, Indira & Williams, Katherine S. 'Draft Cyber-Crime Convention: Criminalisation and the Council of Europe (Draft) Convention on Cyber-Crime', *Computer Law and Security Report*, vol. 18 2(2002): 82-90.

Charlesworth, Andrew. 'Legislating against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990', *Journal of Law and Information Science*, 1(1993): 80-93.

Chang, Lennon Yao-Chung. *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait*, Cheltenham, UK· Northampton, MA, USA: Edward Elgar Publishing, 2012.

Chang, Weiping, Chung, Wingyan, Chen, Hsinchun & Chou, Shichieh 'An International Perspective on Fighting Cybercrime', *Intelligence and Security Informatics*, Lecture Notes in Computer Science vol. 26 65 (2003): 379-384.

Chen, Chunlong. '中国司法解释的地位与功能' (The Status and Function of China's Judicial Interpretation), *Zhongguo Faxue* (China Legal Science), vol. 111 1(2003): 24-32.

Chen, Lihua. '计算机犯罪及立法探讨' (The Discussion on Computer Crime and Its Legislation), *Faxue* (Legal Science), 1(1990): 42-44.

Chen, Jiemiao. '关于我国网络犯罪刑事管辖权立法的思考' (China's Legislation on Jurisdiction over Cybercrimes), *Xiandai Faxue* (Modern Law Science), vol. 30 3(2008): 92-99.

Choo, Kim-Kwang Raymond, Smith, Russell G. & McCusker, Rob. *Future Directions in Technology-enabled Crime: 2007-09*, Canberra, Australia: Australian Institute of Criminology, 2007.

Clough, Jonathan. *Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010.

CNNIC, '第 36 次中国互联网发展状况统计报告（2015 年 7 月）' (The 36th Report on China Information Network Development (July 2015)), available at http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201507/P020150723549500667087.pdf. Last visited November 2015.

Computer Crime and Intellectual Property Section Criminal Division, *Prosecuting Computer Crimes*, published by Office of Legal Education Executive Office for United States Attorneys, 2010.

Coutorie, Larry E. 'The Future of High-Technology Crime: A Parallel Delphi Study', *Journal of Criminal Justice*, vol. 23 1(1995): 13-27.

Dai, Jitao. '从"人肉搜索"看隐私权和言论自由的平衡保护' (Internet Mass Hunting：A Balanced Protection of Privacy and Free Speech), *Faxue* (Legal Research), 11(2008): 40-52.

Darden, Brandon. 'Definitional Vagueness in the CFAA: Will Cyber-bullying Cause the Supreme Court to Intervene?' *Southern Methodist University Science and Technology Law Review*, vol. XIII (2010): 329-358.

Decker, Charlotte. 'Notes, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime', *Southern California Law Review*, vol. 81(2008): 959-1016.

Downing, Richard W. 'Shoring Up the Weakest Link; What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime', *Columbia Journal of Transnational Law*, vol. 43 (2005): 705-762.

Drobnig, Ulrich. 'The Comparability of Socialist and Non-Socialist Systems of Law', *Tel Aviv University Studies in Law*, 3(1977): 45-57.

Endeshaw, Assafa. 'Internet Regulation in China: The Never-ending Cat and Mouse Game', *Information & Communications Technology Law*, 13(2004): 41-57.

Fawzia, Cassim. 'Formulating Specialized Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study', *Potchefstroom Electronic Law Journal*, vol. 12 4(2009): 36-79.

Gercke, Marco. 'Europe's Legal Approaches to Cybercrime', *ERA Forum,* vol. 10 3(2009): 409-420.

Global Internet Policy Initiative. 'Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime', September 2005, available at http://www.internetpolicy.net/cybercrime/20050900cybercrime.pdf. Last visited June 2015.

Goodman, Marc D. 'Why the People Don't Care about Computer Crime?' *Harvard Journal of Law & Technology*, vol. 10 3(1997): 465-494.

Goodman, Marc D. & Brenner, Susan W. 'The Emerging Consensus on Criminal Conduct in Cyberspace', *International Journal of Law and Information Technology*, vol. 10 2(2002): 139-223.

Gordon, Sarah. 'Technologically Enabled Crime: Shifting Paradigms for the Year 2000', *Computer & Security*, vol. 14 5(1995): 391-402.

Griffith, Dodd S. 'The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem', *Vanderbilt Law Review*, vol. 43 3(1990): 453-490.

Hatcher, Michael, McDannell, Jay & Ostfeld, Stacy. 'Computer Crimes', *American Criminal Law Review*, vol. 36 (1999): 397-444.

Heymann, Stephen P. 'Legislating Computer Crime', *Harvard Journal on Legislation*, vol. 34 (1997): 373-391.

Hollinger, Richard C. & Lanza-Kaduce, Lonn. 'The Process of Criminalization: The Case of Computer Crime Laws', *Criminology*, vol. 26 1(1988): 101-126.

Hollinger, Richard C. 'Crime by Computer: Correlates of Software Piracy and Unauthorised Account Access', *Security Journal*, vol. 4 1(1993): 2-12.

Hong, Haeji. 'Hacking Through the Computer Fraud and Abuse Act', *UC Davis Law Review*, vol. 31 (1997): 283-307.

Hopkins, Shannon L. 'Cybercrime Convention: A Positive Beginning to a Long Road Ahead', *Journal of High Technology Law*, vol. II 1(2003): 101-122.

Hu, Ling. '评人肉搜索"第一案"的三个初审判决' (Three First-Instance Judgements of Human Flesh Search Cases), *Internet Law Review*, 1(2012): 181-193.

Huang, Tiayun. '《刑法修正案（七）》解读' (Interpretations on the Amendment (VII) to the Criminal Law), *Renmin Jiancha* (People's Procuratorial), 6(2009): 5-21.

Hunker, Jeffrey. 'U.S. International Policy for Cyber-security: Five Issues that Won't Go away', *Journal of National Security Law and Policy*, 4(2010): 197-216.

Jagatic, Tom N., Johnson, Nathaniel A., Jakobsson, Markus & Menczer, Filippo. 'Social Phishing', *Communications of the Association for Computing Machinery*, vol. 50 10(2007): 94-100.

Jensen, Samantha. 'Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail', *Hamline Law Review,* vol. 36 (2013): 81-138.

Jewkes, Yvonne & Yar, Majid (eds.). *Handbook of Internet Crime* (2nd Edition), Oxford: Routledge, 2011.

Kapitanyan, Matthew. 'Beyound Wargames: How the Computer Fraud and Abuse Act Should Be Interpreted in the Employment Context', *I/S: A Journal of Law and Policy*, vol. 7 1(2011): 405-454.

Kerr, Orin S. 'Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes', *New York University Law Review*, vol. 78 5(2003): 1596-1668.

Kerr, Orin S. 'Vagueness Challenges to the Computer Fraud and Abuse Act', *Minnesota Law Review*, vol. 94 (2009): 1561-1587.

Keyser, Mike. 'The Council of Europe Convention on Cybercrime', *Journal of Transnational Law & Policy*, vol. 12 2(2003): 287-326.

Koops, Bert-Jaap & Brenner, Susan W. (eds.). *Cybercrime and Jurisdiction,* The Hague: T.M.C. Asser Press, 2006.

Lastowka, F. Gregory. & Hunter, Dan. 'Virtual Crimes', *New York Law School Law Review*, vol. 49 (2004): 293-316.

Li, Huaisheng. '论多元化刑事立法模式的构建及方向' (The Diversified Mode of Criminal Legislation and Its Directions), *Shandong Daxue Falv Pinglun* (Law Review of Shandong University), 00(2010): 62-78.

Li, Xiaoming. '刑法："虚拟世界"与"现实社会"的博弈与抉择-从两高"网络诽谤"司法解释说开去'(Criminal Law: Balancing 'the Virtual World' and 'the Real World' – From the perspective of Interpretation of the SPP and SPC on 'cyber insulting'), *Falvkexue* (Science of Law), 2(2015): 119-131.

Liang, Bin & Lu, Hong. 'Internet Development, Censorship, and Cyber Crimes in China', *Journal of Contemporary Criminal Justice*, vol. 26 1(2010): 103-120.

Litman, Harry & Greenberg, Mark D. 'Dual Prosecutions: A Model for Concurrent Federal Jurisdiction', *The ANNALS of the American Academy of Political and Social Science*, vol. 543 1(1996): 72-84.

Liu, Tongfang. '社会学视野中的网络犯罪与综合治理' (Cybercrime and its Comprehensive Regulation-from the perspective of Sociology), *Studies in Dialectics of Nature*, vol. 22 2(2006): 71-74.

Loren, Lydia Pallas. 'Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and the Importance of the Wilfulness Requirement', *Washington University Law Quarterly*, vol. 77 (1999): 835-899.

Lu, Hong, Liang, Bin & Taylor, Melanie. 'A Comparative Analysis of Cybercrimes and Governmental Law Enforcement in China and the United States', *Asian Criminology*, 5(2010): 123-135.

Ma, Qiufeng. '中国计算机犯罪概念探析' (The Concept of Computer Crime), in *The Proceedings of the 7th National Computer Security Conference*, Beijing: China Academic Journal Electronic Publishing House, 1992.

Manacorda, Stefano (ed.). *Cybercriminality: Finding a Balance between Freedom and Security-Selected Papers and Contributions from the International Conference on 'Cybercrime: Global Phenomenon and its Challenges'*, Courmayeur Mont Blanc, Italy, 2-4 December 2011.

Marler, Sara L. 'The Convention on Cybercrime: Should the United States Ratify?' *New England Law Review*, vol. 37 1(2002): 183-219.

Mi, Tienan. '共犯理论在计算机网络犯罪中的困境及其解决方案' (The Dilemmas and Solutions of Accomplice Theories in the Context of Computer Crimes), *Jinan Xuebao* (Jinan Journal), 10(2013): 53-63.

Morris, Sheridan. 'The Future of Netcrime Now: Part 1 – Threats and Challenges', 04(2004): 62 *Home Office Crime and Policing Group*, Washington DC, USA, Tech. Rep.

Nicolai, Seitz. 'Transborder Search: A New Perspective in Law Enforcement', *Yale Journal of Law and Technology*, 7(2004): 23-50.

Nycum, Susan Hubbel. 'The Criminal Law Aspects of Computer Abuse – Part II: Federal Criminal Code', *Journal of Computers and Law*, 5(1976): 297-322.

Olivenbaum, Joseph M. '<Ctrl> <Alt> <Del>: Rethinking Federal Computer Crime Legislation', *Seton Hall Law Review*, vol. 27(1997): 574-641.

Otto, Jan Michiel, Polak, Maurice V., Chen, Jianfu & Li, Yuwen (eds.). *Law-Making in the People's Republic of China*, the Netherlands: Kluwer Law International, 2000.

Parker, Donn B. *Fighting Computer Crime*, New York: Charles Scribner's Sons, 1983.

Phang, Andrew. 'The Singapore Legal System – History, System and Practice', *Singapore Law Review*, vol. 21(2000): 23-61.

Pi, Yong. '我国网络犯罪立法研究-兼论我国刑法修正案七中的网络犯罪立法' (The Study on the Criminal Legislation on Cyber Crimes- the Cybercrime Legislation in the Amendment (VII) to the Criminal Law), *Hebei Faxue* (Hebei Law Science), 6(2009): 49-57.

Pi, Yong. '关于中国网络犯罪刑事立法的研究报告' (Report on China's Criminal Law on Cybercrime), *Xingfa Luncong* (Criminal Law Review), vol. 27 3(2011): 198-257.

Picotti, Lorenzo & Salvadori, Ivan. 'National Legislation implementing the Convention on Cybercrime – Comparative analysis and good practices', *Strasbourg*: Council of Europe, 28 August 2008.

Pocar, Fausto. 'New Challenges for International Rules against Cybercrime', *European Journal on Criminal Policy and Research*, 10(2004): 27-37.

Pollaro, Greg. 'Display Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope', *Duke Law and Technology Review*, 12 (2010): i.

Qu, Cuewu. '因特网上的犯罪及其遏制' (Crimes in Cyberspace and Its Regulation), *Faxue Yanjiu* (Legal Research), 4(2000): 83-100.

Roddy, John. 'The Federal Computer Systems Protection Act', *Journal of Computers, Technology and Law*, 7(1976): 343-365.

Sacco, Rodolfo. 'Legal Formants: A Dynamic Approach to Comparative Law (Installment I of II)', *the American Journal of Comparative Law*, vol. 39(1991): 1-34.

Schjølberg, Stein & Hubbard, Amanda M. 'Harmonizing National Legal Approaches on Cybercrime', *Geneva: International Telecommunication Union (Document: CYB/04) (10 June 2005)*.

Shen, Yuzhong. '个人信息保护与刑法干预的正当性-兼评刑法修正案七第七条' (The Protection to Personal Information and the Legitimacy of Criminal Intervention-the Comments on Article 7 of

Amendment (VII) to Criminal Law), *Journal of Yanshan University (Philosophy and Social Science Edition)*, 6(2009): 84-87.

Sieber, Ulrich. 'Legal Aspects of Computer-related Crime in the Information Society: COMCRIME-Study', *prepared for the European Commission*, 1 January 1998, pp. 19-21.

Skibell, Reid. 'Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act', *Berkeley Technology Law Journal*, vol. 18 (2003): 909-944.

Smith, Russell G., Grabosky, Peter & Urbas, Gregor. *Cyber Criminals on Trial*, Cambridge: Cambridge University Press, 2004.

Smith, Breana C., Ly, Don & Schmiedel, Mary. 'Intellectual Property Crimes', *American Criminal Law Review*, vol. 43 (2006): 663-713.

Sun, Hongyou. '"人肉搜索"中隐私权的保护' (Privacy Protection in Human Flesh Search), *Internet Law Review*, 2(2012): 232- 248.

Taber, John K. 'On Computer Crime (Senate Bill S. 240)', *Computer/Law Journal,* 1(1978-1979): 517-543.

Taylor, Robert W., Fritsch, Eric J., & Liederbach, John. *Digital Crime and Digital Terrorism* (3rd edition), New York: Prentice Hall Press, 2014.

Thaw, David. 'Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement', *The Journal of Criminal Law and Criminology*, vol. 103 3(2013): 907-948.

Toren, Peter J. *Intellectual Property and Computer Crimes*, New York: Law Journal Press, 2014.

Tuma, Shawn E. '"What Does CFAA Mean and Why Should I Care?" – A Primer on The Computer Fraud and Abuse Act for Civil Litigators', *South Carolina Law Review*, vol. 63 (2011): 141-189.

Urbas, G. & Choo, K. R. 'Resource Materials on Technology-Enabled Crime', *Technical and Background Paper no. 28 (AIC, 2008)*.

US Department of Justice, Computer Crime and Intellectual Property Section. *The National Information Infrastructure Protection Act of 1996*, Legislative Analysis (1996).

Weber, Amalie M. 'The Council of Europe's Convention on Cybercrime', *Berkeley Technology Law Journal*, vol. 18 (2003): 425-449.

Westland, Chris. 'A Rational Choice Model of Computer and Network Crime', *International Journal of Electronic Commerce*, vol. 1 2(1996): 109-126.

Wong, Kam C. *Cyberspace Governance in China*, New York: Nova Science Publishers, 2011.

Wong, Mary W. S. 'Cyber-trespass and 'Unauthorised Access' as Legal Mechanisms of Access Control: Lessons from the US Experience', *International Journal of Law and Information Technology*, vol. 15 1(2006): 90-128.

Wu, Dahua. '计算机犯罪的原因，趋势及其综合防范' (The Causes, Features and Tendency of Computer Crime and Its Prevention), *Journal of Guizhou Ethic Institute (Philosophy and Social Science)*, vol. 72 2(2002): 54-61.

Wu, Mengshuan & Luo, Qingdong. *刑法立法修正通用解释* (Common Explanations of the Legislative Interpretation on the Criminal Law), Beijing: China Procuratorate Press, 2002.

Xiong, Wenqi. '人肉搜索浅析' (Analysis on Human Flech Search), *Jiangxi Gongan Zhuanke Xuexiao Xuebao* (Journal of Jiangxi Public Security College), 1(2009): 126-128.

Yang, Xinjing. '刑法与治安管理处罚法竞合问题研究' (The Contradiction between Criminal Law and Public Security Administration Punishments Law), *Renmin Jiancha* (People's Procuratorate), 5(2007): 26-28.

Yu, Haisong. '《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》的理解与适用' (The Understanding and Application of Interpretation of the SPC and the SPP of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems), *Renmin Sifa (Yingyong) (*People's Judicature (Application)), 19(2011): 24-32.

Yu, Zhigang. *网络犯罪定性争议与学理分析* (Analysis on the Nature of Network Crimes), Jilin: Jilin Renmin Chubanshe, 2001.

Yu, Zhigang. '关于使用盗窃行为在网络背景下入罪化思考' (Considerations on 'Usibility Theft' in the Context of Network), *Journal of Beijing Union University* (Humanities and Social Sciences), vol. 5 3(2007): 119-128.

Yu, Zhigang. '网络空间中培训黑客技术行为的入罪化' (The Criminalisation of Training Hackers in Cyberspace), *Yunnan Daxue Xuebao Faxue Ban* (Law Edition Journal of Yunnan University), 1(2010): 86-95.

Yu, Zhigang. '网络犯罪与中国刑法应对' (Cyber Crimes and Chinese Criminal Response), *Zhongguo Shehui Kexue* (Social Science in China), 3(2010): 109-126.

Yu, Zhigang, '三网融合背景下刑事立法的调整方向' (The Direction of the Criminal Law Legislation in the Context of the Combination of Internet, Telecommunication Network and Television Network), *Faxue Luntan* (Legal Forum), 7(2012): 5-12.

Yu, Zhigang. '网络思维的演变与网络犯罪的制裁思路' (The Evolution of Cyber Thinking and the Punishment of Cybercrime), *Peking University Law Journal*, 4(2014): 1045-1058.

Zagaris, Bruce. *International Penal Law Association Report on Information Society, Section 4, United States Report*, 8 January 2013. Available at http://www.penal.org/sites/default/files/files/RH-16.pdf. Last visited March 2015.

Zhang, Mingkai. *刑法学* (Criminal law), Beijing: China Law Press, 2011.

Zhang, Jianjun. '论空白罪状的明确性' (An Analysis on the Clarity of Blank Elements of Criminal Offences), *Faxue* (Legal Science), 5(2012): 139-148.

Zhao, Bingzhi & Yu, Zhigang. '计算机犯罪及其立法和理论之回应' (Computer Crime and the Response from Legislation and Legal Theory), *China Legal Science*, 1(2001): 148-163.

Summary

The development of information technology and digital devices provides new opportunities to crimes. For the first, it facilitates traditional crimes such as fraud, and for the second, it breeds new crimes such as hacking. The traditional crimes facilitated by computers and the new crimes bred by computers are the so-called cybercrime in this research. To combat cybercrime, jurisdictions have developed countermeasures in the field of criminal law both at the national and international levels. At the national levels, China, the United States, England and Singapore have all undergone significant reforms to adapt their criminal law. At the international level, the Council of Europe has launched seminars and projects analysing cybercrime and exploring solutions, and has drafted the Convention on Cybercrime. However, the still commonly happened cybercrime indicates the insufficiency of these countermeasures to cybercrime. The main reasons for this insufficiency are the limited coverage of the criminal law, the transitional and the transnational nature of cybercrime, and the inconsistencies among the national cybercrime legislations. In this regard, this research intends to answer the question: *how can the criminal law be adapted to regulate cybercrime?*

In answering this question, this research contains six substantial Chapters apart from the introduction (Chapter 1). These Chapters are structured in two parts: Chapters 2 - 6 explore and analyse cybercrime legislations in the selected five legal regimes both in the past and in the present, and based on these previous explorations and analysis Chapter 7 provides comparison, conclusion and recommendation. To be specific, each of Chapters 2 – 6 investigates the evolvement of cybercrime legislation in a selected legal regime and examines the legislative approaches in addressing the challenges presented by cybercrime. The debate behind these legislative approaches mainly revolves around one balance: promoting the online freedom or enhancing the control over cyberspace. Each of the two sides points to a different way of legislating against cybercrime. In particular, should the society shed a stringent regulation over cyber activities in order to lower the risk of cybercrime, or should they bear the risk so as to promote the freedom in cyberspace? In the end, Chapter 7 draws observations on the legislative processes and approaches in the selected legal regimes, in particular through comparing how these legal regimes strike the balance between online freedom and control and how this balance has influenced the responses to the core contentious issues regarding cybercrime. Following the comparison, Chapter 7 provides the

conclusion of this thesis regarding the legislative approaches a jurisdiction can take to adapt its criminal law to combat cybercrime.

The comparision has shown that cybercrime necessitates a systematic, comprehensive, and stable legislation. In the initial stage of this legislation, the selected legal regimes had limited its reach. However, they soon noticed the lack of coverage of the legislation and the threat to the national security presented by cybercrime. In the later stage therefore, they all expanded the legislation to certain degrees. In expanding the legislation, these legal regimes have demonstrated divergences with respect to the legislative approaches they take: China and the US take the approach focusing on the function of computer; England once took the approach focusing on the reliability and the confidentiality of data before 2006; and the Council of Europe, England (after 2006) and Singapore take the approach focusing on both. The comparison of these approaches and the experiences in combating cybercrime of the legal regimes manifest the advantages of the last approach in preventing over-incrimination and promoting international harmonisation. This approach includes four steps. Firstly, the cybercrime legislation must distinguish the new crimes targeting computers and the traditional crimes facilitated by computers. Secondly, within the new crimes targeting computers, the legislation must identify and distinguish that both the confidentiality of data and the function of the computer are the targets. Thirdly, each provision in the cybercrime legislation must clarify the interest it intends to protect in order to avoid confusions and overlaps among provisions. In the end, when applying these provisions, judges must identify the subject suffered, i.e. the function of the computer or the reliability and confidentiality of data, and then choose the applicable provision correspondingly.

Samenvatting

De ontwikkeling van de informatietechnologie en digitale apparaten biedt nieuwe kansen voor criminaliteit. Ten eerste vereenvoudigt deze ontwikkeling traditionele criminaliteit zoals fraude en ten tweede leidt deze tot nieuwe vormen van misdaad zoals hacking. De zogeheten cybercriminaliteit in dit onderzoek bestaat uit de traditionele criminaliteit die vergemakkelijkt wordt door het gebruik van computers en de nieuwe criminaliteit die voortkomt uit het gebruik van computers. Om cybercriminaliteit te bestrijden hebben jurisdicties tegenmaatregelen ontwikkeld op het gebied van strafrecht, zowel op nationaal als op internationaal niveau. Op nationaal niveau hebben China, de Verenigde Staten, Engeland en Singapore ingrijpende hervormingen doorgevoerd om hun strafrecht aan te passen. Op internationaal niveau heeft de Raad van Europa seminars en projecten gelanceerd om cybercriminaliteit te analyseren en oplossingen te verkennen en daarnaast het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken opgesteld. Uit het feit dat er nog steeds veelvuldig sprake is van cybercriminaliteit blijkt dat de genoemde tegenmaatregelen op het gebied van cybercriminaliteit ontoereikend zijn. De voornaamste oorzaken van deze ontoereikendheid zijn de beperkte reikwijdte van het strafrecht, het transitionele en transnationale karakter van cybercriminaliteit en de inconsistenties tussen de nationale wetgevingen inzake cybercriminaliteit van verschillende landen. Binnen dit kader is dit onderzoek gericht op het beantwoorden van de volgende vraag: *hoe kan het strafrecht worden aangepast om de cybercriminaliteit te reguleren?*

Na de inleiding (hoofdstuk 1) zal deze vraag in zes uitgebreide hoofdstukken worden beantwoord. Deze hoofdstukken vallen uiteen in twee groepen: In hoofdstuk 2 - 6 wordt de wetgeving inzake cybercriminaliteit, zowel in het verleden als in het heden, verkend en geanalyseerd, uitgaande van de vijf geselecteerde rechtsstelsels. Op basis van deze verkenningen en analyses worden in hoofdstuk 7 vergelijkingen gemaakt, wordt een conclusie getrokken en worden aanbevelingen gedaan. Meer specifiek wordt in hoofdstuk 2 – 6 de ontwikkeling van wetgeving inzake cybercriminaliteit in het geselecteerd rechtsstelsel onderzocht en gekeken naar de manieren waarop de uitdagingen die cybercriminaliteit met zich meebrengt juridisch worden benaderd. In het achterliggende debat over deze juridische

benaderingen draait het voornamelijk om één bepaald evenwicht, namelijk dat tussen het bevorderen van de online vrijheid en het vergroten van de controle over cyberspace. Beide kanten in het debat propageren andere juridische maatregelen gericht tegen cybercriminaliteit. Het gaat hierbij vooral om de vraag of de samenleving cyberactiviteiten aan strenge regels moet onderwerpen om het risico van cybercriminaliteit te verkleinen of dat men dit risico moet aanvaarden ten einde de vrijheid in cyberspace te bevorderen. Tot slot worden in hoofdstuk 7 constateringen gedaan over de wetgevingsprocessen en juridische benaderingen in de geselecteerde rechtsstelsels, met name door te vergelijken hoe deze rechtsstelsels streven naar een evenwicht tussen online vrijheid en regulering van internet en hoe dit evenwicht van invloed is op de manier waarop wordt ingespeeld op de belangrijkste vraagstukken met betrekking tot cybercriminaliteit. Volgend op deze vergelijking bevat hoofdstuk 7 de conclusie van dit proefschrift met betrekking tot de juridische benaderingen die een rechtsstelsel kan hanteren om zijn strafrecht aan te passen teneinde cybercriminaliteit te bestrijden.

Uit de vergelijking komt naar voren dat cybercriminaliteit een systematische, alomvattende en stabiele wetgeving noodzakelijk maakt. In de eerste fase van deze wetgeving was het toepassingsgebied van de wetgeving in de geselecteerde rechtsstelsels beperkt. Er werd echter al snel vastgesteld dat de wetgeving onvoldoende reikwijdte had en cybercriminaliteit de nationale veiligheid in gevaar bracht. In een latere fase werd de wetgeving in alle rechtsstelsels derhalve in zekere mate uitgebreid. Bij het uitbreiden van de wetgeving in deze rechtsstelsels blijken verschillen op te treden met betrekking tot de gekozen juridische benaderingen: China en de VS richten zich in hun benadering op de functie van de computer; Engeland koos vóór 2006 aanvankelijk voor een benadering waarbij het draaide om de betrouwbaarheid en vertrouwelijkheid van gegevens; de Raad van Europa, Engeland (na 2006) en Singapore doen in hun benadering beide. De vergelijking van deze benaderingen en de ervaringen die in de rechtsstelsels zijn opgedaan bij de bestrijding van cybercriminaliteit duiden op de voordelen van de laatstgenoemde benadering bij het voorkomen van te vergaande strafbaarstelling en het bevorderen van internationale harmonisering. Deze benadering bestaat uit vier stappen. Ten eerste dient in de wetgeving inzake cybercriminaliteit onderscheid te worden gemaakt tussen de nieuwe criminaliteit met computers als doelwit en de traditionele criminaliteit die wordt vergemakkelijkt door computers. Ten tweede moet de wetgeving vaststellen en onderkennen dat, ten aanzien van de nieuwe criminaliteit met computers als doelwit, zowel de

vertrouwelijkheid van gegevens als de functie van de computer doelwit is. Ten derde dient in iedere bepaling in de wetgeving inzake cybercriminaliteit te worden duidelijk gemaakt welk belang wordt beschermd om verwarring en elkaar overlappende bepalingen te vermijden. Bij de toepassing van deze bepalingen dienen rechters uiteindelijk vast te stellen wat er in gevaar is, d.w.z. de functie van de computer of de betrouwbaarheid en vertrouwelijkheid van gegevens, en vervolgens dienovereenkomstig de geldende bepaling te kiezen.

Curriculum vitae

Qianyun WANG
Susan32100@hotmail.com

Short bio

Qianyun WANG started her research as a PhD candidate of Erasmus School of Law in September 2012. Before coming to the ESL, she studied for her Bachelor Degree in Southwest University of Political Science and Law in China from 2006 to 2010. After four years' studying in law, she went on for a Master Degree in China University of Political Science and Law, majored in Criminal Law. Because of her outstanding performance, she managed her Master Degree in two years, one year earlier than the required three years. During studying for Mater Degree, she took part in two internship programs, organised by Google (China) for 8 months and by the Supreme People's Court for 4 months respectively.

As a PhD candidate, Qianyun WANG is co-supervised by Prof. Yuwen Li from Erasmus China Law Centre and Prof. Paul Mevis from the Criminal Law Department. She is doing a comparative research on cybercrime in the field of criminal law, including China, US, UK, Singapore and the Council of Europe. Specifically, she focuses on the legislative approaches the criminal law takes to combat cybercrime in these five legal regimes, intending to examine the convergences and divergences among the countermeasures to cybercrime in these legal regimes, and explore possible legislative approaches to adapt the criminal law.

During pursuing her PhD degree, she managed to publish one article on death penalty of fraudulent fundraising in China, and participated in a translation project sponsored by the Encyclopaedia of China Publishing House – 'Foreign Scholars on Chinese Law', mainly responsible for the Issue on the criminal procedural law. This Issue is currently under proofreading, and will be published soon.

Education	
Southwest University of Political Science and Law	2006-2010
China University of Political Science and Law	2010-2012
Erasmus University Rotterdam	2012-2016
Work experience	
Supreme People's Court of China	2011
Google (China)	2011-2012
Prizes and awards	
Scholarship of China Scholarship Council	2012-2016
Publications	
'The Death Penalty's Survival and Application for the Crime of Fraudulent Fundraising in China', in *Onbegrensd Strafrecht*, Oisterwijk, the Netherlands: Wolf Legal Publishers.	2013
(translation) 'Foreign Scholars on Chinese Law – Issue on the Criminal Procedural Law'	Forthcoming

PhD Portfolio

Name PhD student : Qianyun WANG
PhD-period : Sep. 2012 – Dec. 2016
Promoters : Prof. Yuwen Li and Prof. Paul Mevis

PhD training

EGSL courses	*year*
Reflection on Social Science	2013
How to Make Presentation	2013
Writing Clinic	2013
Research Lab	2012
Introduction of Legal Research Method	2012
Academic Writing	2012
Seminars and workshops	*year(s)*
ESL Brown Bag Lunches Lectures	2012-2016
ECLC Brown Bag Lunch Lectures	2012-2016
ESL Poster Presentations	2012-2016
Seminar by Criminology Department of ESL: Justice that Brings out the Good	Jan. 2016

ECLC Seminar by Guest Lecturer Prof. Qing Tianbao on 'New developments of Environmental Law in China'.	Jan. 2015
National PhD day for criminal law PhDs	May 2014
Seminars organized by EGSL Discussing Group on 'Reflection of Social Norms and Legal Norms'.	2014
ECLC Seminar by Guest Lecturer Dr. Zhao Yun on 'New Developments of Dispute Resolution in China'.	May 2013
ECLC Seminar by Guest Lecturer Mr. Mao Yushi on 'Puzzles of the Reform of Economic System in China'.	June 2013
ECLC Seminar by Guest Lecturer Prof. Zhan Zhongle on 'Reform on China's Administrative Litigation System'.	June 2013
Workshop of Legal PhD Candidates in the Netherlands	Oct. 2013
Presentations	*year*
ECLC Brown Bag Lecture (every three months): presenting the latest work.	2013-2016
ESL Brown Bag Lunch The Amendment (IX) to the Criminal Law of China	2015
2014 Annual Conference: Cyberspace The Process of Criminalizing Computer Misuses – the ideology behind	2014
Attendance (international) conferences	*year*
Computers, Privacy & Data Protection, organised by Free University of Brussels and Tilburg University	2016
Law and Governance in Digital Era, organised by the Netherlands Institute for Law and Governance	2015
2014 Annual Conference Cyberspace, organised by Masaryk University and European Academy of Law and ICT	2014
Cybercrime Conference: Social Science Perspectives, organized by Criminology Department of ESL	2014

2013 Annual Conference Cyberspace, organised by Masaryk University and European Academy of Law and ICT	2013
Others	*year*
International Criminal Court Moot Court Competition	2015
Sino-Dutch Lawyers Visiting Programme	2013-2014
Sino-Dutch Public Interests Lawyers Training Programme	2013