

Contents

Part I Fundamentals of Cybercrime

1	Cybercrime: Introduction, Motivation and Methods	3
1.1	Introduction	3
1.1.1	Definition	3
1.1.2	Contemporary Cybercrime	7
1.1.3	Terrestrial Crimes Versus Cybercrimes	7
1.1.4	Cybercrime and White Collar Crime	8
1.2	The Scale of the Problem and Reasons for the Growth of Cybercrime	9
1.2.1	United States	10
1.2.2	United Kingdom	11
1.2.3	Middle East	12
1.2.4	Asia/Pacific—Japan (APJ)	13
1.3	Profiling Cybercriminals	15
1.3.1	Motives of the Cybercriminal	15
1.3.2	How Cybercriminals Use the Network	15
1.3.3	Types of Cyber Criminals	16
1.4	Challenges for Criminal Justice and Law Enforcement	20
1.4.1	Transnational Legal Jurisdictions	20
1.4.2	Evidence Identification and Tracking	20
1.4.3	Tactics for Evasion	21
1.5	The Future of Cybercrime	21
1.6	Summary	22
	References	23

Part II Computer System as Target

2	Unauthorized Access Offences in Cyberworld.	27
2.1	Emerging Threats: Expected Targets and Forms	27
2.2	Criminal Statues	29
2.2.1	United States	29
2.2.2	United Kingdom	32
2.3	Other Offences Associated with Hacking	34
2.3.1	Unauthorized Modification of Computer Programs or Data	34
2.3.2	Computer Viruses	36
2.4	Summary	37
	References.	37
3	Injection of Malicious Code in Application.	39
3.1	Introduction	39
3.2	Types of Malicious Code	40
3.2.1	File Infector Viruses	40
3.2.2	Boot Sector Viruses	41
3.2.3	Macro Viruses	41
3.2.4	Worms	42
3.2.5	Trojan Horses	42
3.3	Threats Posed by Viruses, Worms, and Trojan Horses	43
3.3.1	Data Corruption and Loss	43
3.3.2	Data Theft	44
3.3.3	Stuxnet Worm	45
3.3.4	The Number of Threats	46
3.4	Legislative Approaches	47
3.4.1	The American Approach	47
3.4.2	The Council of Europe Convention on Cybercrime	48
3.5	Summary	50
	References.	51

Part III Computer System as Tool

4	Attempts and Impact of Phishing in Cyberworld	55
4.1	The Problem of Phishing	55
4.2	Impact and Harm Generated by Phishing	56
4.3	Mechanisms of Cyberspace Phishing	58
4.3.1	Dragnet Method	58
4.3.2	Rod—and—Reel Method	58
4.3.3	Lobsterpot Method	59
4.3.4	Gillnet Phishing	59
4.3.5	Political Phishing	60

4.4	Using Stolen Financial Information	61
4.5	Customer Vigilance.	62
4.6	Summary	63
	References.	63
5	Sexual Harassment in Cyberworld.	65
5.1	Introduction	65
5.2	Harassment in Cyberworld	66
5.3	Cases and Prevalence of Sexual Harassment in Cyberspace	68
5.4	Enforcement Problems.	69
5.4.1	The International Stalker	69
5.4.2	The Anonymous Stalker	69
5.5	Legal Regulation	70
5.5.1	United States	71
5.5.2	United Kingdom.	73
5.6	Non Legal Regulation	74
5.6.1	Software	74
5.6.2	Education of Internet Users	75
5.6.3	Internet Service Providers	75
5.7	Prevention of Sexual Harassment on the Internet	75
5.7.1	Legislation and Law Enforcement.	76
5.7.2	Changing the Culture and Norms	76
5.7.3	Educating Potential Victims and Harassers.	76
5.8	Summary	77
	References.	77

Part IV Content-Related Offenses

6	Online Obscenity and Child Sexual Abuse	81
6.1	Introduction	81
6.2	The Role of the Internet in Promoting Child Sexual Abuse	82
6.2.1	Production of Pornographic Content	83
6.2.2	Distribution and Sharing	83
6.2.3	Consumption of Pornographic Content	86
6.3	Criminal Offenses Against Children	86
6.3.1	Cybering	86
6.3.2	Online Grooming	88
6.3.3	Age Play	89
6.3.4	Exposure to Online Obscenity	89
6.4	Minimizing Risks	91
6.5	Where Next?	92
	References.	93

Part V Privacy, Security and Crime Control

7	Anonymity, Privacy and Security Issues in Cyberworld	97
7.1	Introduction	97
7.2	Anonymity in Cyberspace	98
7.2.1	True Anonymity	98
7.2.2	Pseudo-Anonymity	99
7.2.3	Anonymity, Privacy and Freedom of Speech	99
7.3	Impact and Harm Generated by Anonymity	101
7.4	Regulating Anonymity in Cyberspace	103
7.5	The Case Law	108
7.5.1	Al Farhan Case	108
7.5.2	Bin Saleh Case	108
7.6	The Appropriate Balance	109
7.7	Summary	109
	References.	110
8	Strategies and Statutes for Prevention of Cybercrime	113
8.1	Introduction	113
8.2	National and Regional Strategies: The European Approach	114
8.2.1	The Council of Europe Convention on Cybercrime	115
8.3	The American Response	118
8.3.1	Communication Interference Statute	118
8.3.2	The Stored Communications Act (SCA)	118
8.3.3	Wiretap Act	119
8.3.4	Wire Fraud Statute	120
8.3.5	Can-Spam Act	121
8.3.6	Other Federal Statutes Related to Cyber Security	121
8.4	Technical Approach	124
8.5	The Future	125
8.6	Summary	125
	References.	126
9	419 Scam: An Evaluation of Cybercrime and Criminal Code in Nigeria	129
9.1	The Meaning of 419 Scam.	129
9.2	The Operation of the Scheme	130
9.3	The Nature and Extent of the Problem.	131
9.4	Evaluation of the Current Situation in Nigeria	132
9.5	419 Scam Combating Efforts in Nigeria.	133
9.5.1	Legislative Approaches	133
9.5.2	Administrative Measures	137
9.5.3	Technical Measures.	140
9.6	The Quest for Legislative Harmonisation	142

Contents	xv
9.7 Future Trends.	143
9.8 Summary	143
References.	144
Appendix	145



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

Cybercrime, Digital Forensics and Jurisdiction

Chawki, M.; Darwish, A.; Khan, M.A.; Tyagi, S.

2015, XVIII, 145 p., Hardcover

ISBN: 978-3-319-15149-6