ÍNDICE

Pág.

PRÓLOGO, por *Marcus Felson* 13

PREÁMBULO Y AGRADECIMIENTOS 17

ABREVIATURAS 21

INTRODUCCIÓN 25

PRIMERA PARTE
FENOMENOLOGÍA DEL CIBERCRIMEN

CAPÍTULO I
LA CRIMINALIDAD EN EL CIBERESPACIO:
LA CIBERCRIMINALIDAD

1. ACERCA DE LOS CONCEPTOS CIBERCRIMEN Y CIBERCRIMINALIDAD 33
   1.1. De la delincuencia informática a la cibercriminalidad: evolución de un término por la evolución del fenómeno 34
   1.2. El cibercrimen: sentidos tipológico y normativo, concepciones amplia y restringida, y relación con el término cibercriminalidad 39
2. EL CIBERCRIMEN: FUNCIONES DE LA CATEGORÍA Y CONCEPCIÓN AMPLIA DEL CIBERCRIMEN 43

CAPÍTULO II
TIPOS DE CIBERCRIMEN Y CLASIFICACIÓN
DE LOS MISMOS

1. INTRODUCCIÓN: EL CIBERCRIMEN (LOS CIBERCRÍMENES) 47

Pág.

2. CLASIFICACIÓN ATENDIENDO A LA INCIDENCIA DE LAS TIC EN EL COMPORTAMIENTO CRIMINAL 51
2.1. Ciberataques puros 52
2.1.1. El *hacking* 53
2.1.2. Infecciones de *malware* y otras formas de sabotaje cibernético 57
2.1.2.1. *Malware* 59
2.1.2.2. Sabotaje de *insiders* 62
2.1.2.3. Ataques DoS 62
2.1.2.4. *Spam* 66
2.1.3. Ocupación o uso de redes sin autorización 67
2.1.4. *Antisocial networks* 67
2.2. Ciberataques réplica 68
2.2.1. Los ciberfraudes (*auction fraud* y otros) 69
2.2.1.1. Los ciberfraudes burdos o *scam* 71
2.2.1.2. El *phishing* 72
2.2.2. *Identity theft* y cibersuplantación de identidad o *spoofing* 79
2.2.3. El ciberespionaje 81
2.2.4. Ciberblanqueo de capitales y ciberextorsión 83
2.2.5. El ciberacoso 84
2.2.5.1. El *cyberbullying* o acoso escolar o a menores en Internet 85
2.2.5.2. El *cyberstalking* (y el *online harassment*) 88
2.2.5.3. El ciberacoso sexual, el *sexting*, el *online grooming* 92
2.3. Ciberataques de contenido 100
2.3.1. La ciberpiratería intelectual 102
2.3.2. Pornografía infantil en Internet 106
2.3.3. Difusión de otros contenidos ilícitos (especial atención al *online hate speech* o difusión por Internet de odio racial) 113

3. OTRA CLASIFICACIÓN ES POSIBLE: ATENDIENDO AL MÓVIL Y CONTEXTO CRIMINOLÓGICO 116
3.1. El cibercrimen económico: la simbiosis de los ciberataques con finalidad económica 119
3.2. El cibercrimen «social» en la web 2.0: redes sociales, desarrollo de la personalidad en el ciberespacio y nuevos cibercrímenes 122
3.3. El cibercrimen político: ciberterrorismo, *hacktivismo*, y otras formas de delincuencia política en el ciberespacio 127
3.3.1. El ciberterrorismo 127
3.3.2. La ciberguerra 133
3.3.3. El ciberhacktivismo 135

Pág.

SEGUNDA PARTE
CRIMINOLOGÍA DEL CIBERCRIMEN

CAPÍTULO III
CIBERESPACIO Y OPORTUNIDAD DELICTIVA

1. INTRODUCCIÓN 143
2. ARQUITECTURA DEL CIBERESPACIO 145
2.1. Tiempo y espacio en el ciberespacio 146
2.2. El ciberespacio transnacional, universal, neutro, abierto al cambio, etcétera 152
2.2.1. El ciberespacio transnacional 153
2.2.2. La neutralidad en la Red 155
2.2.3. El ciberespacio no centralizado (más bien distribuido) 155
2.2.4. La universalidad y popularización del ciberespacio 157
2.2.5. El ciberespacio anonimizado 157
2.2.6. El ciberespacio, sujeto a revolución permanente y abierto al cambio 158

3. ¿ES EL CIBERESPACIO UN NUEVO ÁMBITO DE RIESGO DELICTIVO? LA OPORTUNIDAD DELICTIVA EN EL CIBERESPACIO 161
3.1. Introducción: teoría criminológica y cibercrimen 161
3.2. El triángulo del cibercrimen: el ciberespacio, nuevo ámbito de oportunidad criminal 168
3.2.1. El ciberagresor motivado 170
3.2.2. Objetivos adecuados en el ciberespacio: del VIVA al IVI 179
3.2.3. Guardianes capaces y gestores del lugar «ciberespacio» 187

4. OPORTUNIDAD DELICTIVA EN EL CIBERESPACIO Y PREVENCIÓN DEL CIBERCRIMEN 191
4.1. La importancia de la víctima en el evento «cibercrimen» 191
4.2. De las actividades cotidianas a la prevención (situacional) del cibercrimen 194
4.3. La prevención del cibercrimen y el enfoque situacional 203
4.3.1. Medidas concretas para la prevención del cibercrimen desde el enfoque «situacional» 203
4.3.2. Alcance y limitaciones del enfoque situacional: el desplazamiento (mejor adaptación) del cibercrimen 216

CAPÍTULO IV
EL CIBERCRIMINAL. PERFILES DE DELINCUENTES EN EL CIBERESPACIO

1. BESTIARIO DEL CIBERESPACIO 229

Pág.

1.1. Introducción: del *hacker* cinematográfico al «cibercriminal común». 229
1.2. Los *hackers* (y dentro de la categoría, también *crackers, script-kiddies,* etc.) ... 231

2. ESPECIALIDADES DEL PERFIL DEL CIBERCRIMINAL DERIVADAS DE LA MODALIDAD DE CIBERCRIMEN REALIZADO ... 237

2.1. El cibercriminal económico ... 237

2.1.1. No sólo *hackers*: también insiders y especialmente grupos organizados ... 238
2.1.2. Perfil del cibercriminal económico: ¿delincuente común, de cuello blanco, socioeconómico o universitario? La cuestión de la tecnificación del cibercriminal económico... 245

2.2. *Ciberhacktivistas,* ciberterroristas y demás cibercriminales políticos ... 250
2.3. El cibercriminal social ... 253

2.3.1. El *cybergroomer* ... 254
2.3.2. El *cyberstalker* ... 256
2.3.3. El *cyberbulliy* ... 258

CAPÍTULO V

LA CIBERVÍCTIMA: PERFILES DE VICTIMIZACIÓN Y RIESGO REAL DE LA AMENAZA DEL CIBERCRIMEN

1. INTRODUCCIÓN: MULTIPLICIDAD DE CIBERCRÍMENES = MULTIPLICIDAD DE CIBERVÍCTIMAS ... 261
2. LA VICTIMIZACIÓN EN EL CIBERESPACIO: CONSIDERACIONES GENERALES DE NUEVO DESDE EL PRISMA DE LAS ACTIVIDADES COTIDIANAS ... 263
3. ANÁLISIS DE ALGUNOS ÁMBITOS ESPECÍFICOS DE VICTIMIZACIÓN ... 270

3.1. Comercio y banca electrónica y victimización frente al cibercrimen.. 270
3.2. Redes sociales y demás medios de intercomunicación social en el ciberespacio ... 271

3.2.1. Conducta de la víctima y cibercriminalidad social ... 271
3.2.2. Los menores como víctimas de la cibercriminalidad social en el ciberespacio ... 275

4. ENTRE LA EXAGERACIÓN Y LA BANALIZACIÓN: CIFRA NEGRA Y REALIDAD DE LA AMENAZA DEL CIBERCRIMEN ... 288

GLOSARIO ... 299
ÍNDICE DE TABLAS ... 311
ÍNDICE DE ILUSTRACIONES ... 313
BIBLIOGRAFÍA ... 315