



MINISTERIO DE DEFENSA

CUADERNOS
de
ESTRATEGIA

149

**CIBERSEGURIDAD.
RETOS Y AMENAZAS A LA SEGURIDAD
NACIONAL EN EL CIBERESPACIO**

INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS
INSTITUTO UNIVERSITARIO «GENERAL GUTIÉRREZ MELLADO»

ÍNDICE

	<i>Página</i>
SUMARIO	5
PRESENTACIÓN	9
INTRODUCCIÓN	11
<i>Capítulo I</i>	
ÁLCANCE Y ÁMBITO DE LA SEGURIDAD NACIONAL EN EL CIBERESPACIO	47
Introducción	50
Ciberespacio: Definiciones e implicaciones.....	53
– Definiciones	53
– Implicaciones.....	55
La seguridad del ciberespacio en el ámbito español.....	58
– Consideraciones normativas	58
– Cómo se gestiona la seguridad en España	60
El ámbito europeo, de la OTAN y el norteamericano	66
– La Unión Europea	66
– El marco OTAN	68
– USA.....	68

	<u>Página</u>
Tipos ataques y atacantes	70
– Tipos de ataques	70
– Tipos de atacantes	71
– Evolución de los ciberataques.....	73
– La amenaza a las Infraestructuras Críticas.....	75
Necesidad de estrategias de ciberseguridad.....	77
Conclusiones.....	80
Bibliografía	81

Capítulo II

ESTRATEGIAS LEGALES FRENTE A LAS CIBERAMENAZAS	83
El punto de partida. la expansión del concepto de seguridad nacional: ciberdelitos y ciberamenazas	86
– La expansión del concepto de seguridad nacional.....	86
– Nuevos escenarios, nuevas amenazas, nuevas respuestas.....	89
– Ciberdelitos y ciberamenazas.....	92
Las respuestas del sistema legal	98
– Grandes líneas de la situación a escala mundial.....	98
– Convenio del Consejo de Europa, sobre cibercriminalidad.....	99
– Otros instrumentos normativos de la Unión Europea.....	102
– Criminalidad organizada y terrorismo	104
– Derecho penal español	105
Un balance del debate jurídico actual.....	108
– Categorías Generales	108
– Problemas Específicos	115
Conclusiones.....	119
Bibliografía	121

Capítulo III

EL CIBERESPACIO Y EL CRIMEN ORGANIZADO	129
Introducción	132
El delito informático.....	135
Del Hacker Romántico al Pirata Informático	138
Hacking by dollar?	142

	<u>Página</u>
La delincuencia organizada	143
– Fraude en comercio electrónico	144
• El carding	145
• Las ventas en portales de anuncios clasificados.....	146
– Fraude en banca electrónica	150
– Crime as a service	155
– La infraestructura de mulas	159
– Los timos en la red	162
Bibliografía	164

Capítulo IV

LA SITUACIÓN DE LA CIBERSEGURIDAD EN EL ÁMBITO INTERNACIONAL Y EN LA OTAN.....	165
Introducción	168
La ciberseguridad en el ámbito internacional	171
El ciber caso Estonia 2007	174
– Antecedentes.....	174
– Cronología de los ciber ataques.....	178
– Tipos de ataques	180
– Objetivos.....	184
– La respuesta técnica.....	186
– La respuesta política.....	188
– La respuesta legal.....	191
– Investigación forense.....	193
– Conclusiones	194
El ciber caso Georgia 2008	195
– Antecedentes.....	196
– Cronología de los ciber ataques.....	197
– Tipos de ataques	198
– Objetivos.....	199
– La respuesta técnica.....	200
– La respuesta política.....	200
– La respuesta legal.....	200
– Investigación forense.....	201
– Conclusiones	202

	<u>Página</u>
La ciberseguridad en la OTAN.....	202
– La Ciberdefensa en la OTAN.....	204
– La amenaza cibernética y el artículo 4 del tratado de Washington...	208
– La amenaza cibernética y el artículo 5 del tratado de Washington...	208
– La amenaza cibernética y el artículo 6 del tratado de Washington...	212
– Conclusiones	213
Bibliografía	213
 <i>Capítulo V</i>	
LA CIBERSEGURIDAD EN EL ÁMBITO MILITAR.....	215
Introducción	218
– Escenario estratégico general	219
– El ciberespacio y la ciberseguridad	220
– Las operaciones cibernéticas en redes (CNO; Computer Network Operations)	227
– NNEC (NATO Network Enabled Capability).....	228
– Revisión del concepto estratégico de la OTAN. Ciberespacio y el artículo V.....	231
– La Amenaza	231
– Ataques e incidentes reseñables.....	235
– EEUU	235
– Estonia.....	236
Organización de la seguridad de la información y normativa en el Ministerio de Defensa.....	238
Infraestructura. ámbitos de propósito general y mando y control ...	243
– Plan Director CIS	243
Cooperación internacional.	245
Formación y adiestramiento.....	246
– Sensibilización, Concienciación y Formación.	246
– Ejercicios de ciberdefensa.....	248
Cifra.....	249
Conclusiones.....	250
Bibliografía	254

Capítulo VI

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD. CIBER-TERRORISMO	257
Introducción	260
Agentes de la amenaza	263
– Ciberterrorismo	265
– Ciberespionaje	269
Infraestructuras críticas	270
– Centro Nacional de Protección de Infraestructuras Críticas	271
– Catálogo de Infraestructuras Críticas	272
– Plan de Protección de Infraestructuras Críticas	272
– Ciberataques en las Infraestructuras Críticas	273
• Sistemas SCADA	274
Estrategias nacionales de ciberseguridad en otros países	274
– Estados Unidos	275
– Reino Unido	281
– Canadá	284
– Francia	285
– Alemania	287
– Estonia	289
– Australia	290
– Organizaciones Internacionales	294
– Conclusiones	294
España. responsabilidades en el ciberespacio	295
– Ministerio de Industria Turismo y Comercio	296
– Ministerio del Interior	297
– Ministerio de Política Territorial y Administración Pública	297
• Consejo Superior de Administración Electrónica	298
– Centro Nacional de Inteligencia	299
• Oficina Nacional de Seguridad	299
• Centro Criptológico Nacional	299
– Ministerio de Defensa	300
• Dirección General de Infraestructuras	301
• Estado Mayor de la Defensa	301
• Cuarteles Generales	301

	<u>Página</u>
– Equipos de Respuesta ante Incidentes	301
• Relaciones internacionales	304
España. situación actual	305
– Ámbitos de actuación en ciberseguridad	306
– Sistemas Clasificados	307
– Esquema Nacional de Seguridad	308
– Protección de Datos personales.....	311
– Sistemas asociados a Infraestructuras críticas	312
Estrategia española de ciberseguridad.....	312
– Objetivos.....	312
– Líneas estratégicas de acción	313
– Posible estructura de la ciberseguridad	315
Conclusiones.....	317
Bibliografía	318
CONCLUSIONES	323
 <i>Anexo A</i>	
LÍNEAS DE ACCIÓN DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD.....	336
 <i>Anexo B</i>	
GLOSARIO.....	345
COMPOSICIÓN DEL GRUPO DE TRABAJO	353