LUCÍA MILLÁN MORO
Directora
GLORIA FERNÁNDEZ ARRIBAS
Editora

Ciberataques y ciberseguridad en la escena internacional

Mª TERESA ACEYTUNO PÉREZ
Mª DEL ROSARIO CARMONA LUQUE
GUILLEM COLOM PIELLA
JOSÉ MANUEL CORTÉS MARTÍN
ANTONIO LAZARI
JONATHAN PASS
CONCHA PÉREZ CURIEL
LUIS PÉREZ-PRAT DURBÁN
MANUEL RICARDO TORRES SORIANO
RAMSES A. WESSEL

THOMSON REUTERS
ARANZADI

Índice General

Página

PARTE I

CAPÍTULO 1

LOS CIBERATAQUES Y EL USO DE LA FUERZA EN LAS RELACIONES INTERNACIONALES 17

LUIS PÉREZ-PRAT DURBÁN

I. Ciberataques y Derecho Internacional 17
II. Algunos casos de ciberataques 23
III. Las normas sobre los ciberataques 31
IV. ¿Pueden los ciberataques ser contemplados como un uso ilegal de la fuerza? 38
V. El ciberataque como ataque armado 44
VI. Conclusiones 49

CAPÍTULO 2

CIBERATAQUES Y RESPONSABILIDAD: SOBRE LAS ASIMÉTRICAS INCERTIDUMBRES DEL DERECHO INTERNACIONAL VIGENTE 51

JOSÉ MANUEL CORTÉS MARTÍN

I. Introducción 51
II. De la incertidumbre en cuanto a las normas primarias 54
1. *Soberanía* 55
2. *No intervención* 57
3. *Diligencia debida* 59
III. De la incertidumbre en cuanto a las normas secundarias: el problema de la atribución del hecho ilícito 61

Página

IV. Conclusiones 68

CAPÍTULO 3

EL PRINCIPIO DE DISTINCIÓN ENTRE CIVILES Y COMBATIENTES Y SU APLICACIÓN A LOS MÉTODOS Y MEDIOS DE COMBATE CIBERNÉTICOS 71

GLORIA FERNÁNDEZ ARRIBAS

I. Retos actuales relativos a las normas y principios de derecho internacional humanitario, con especial atención al principio de distinción 71

II. El principio de distinción aplicado a las guerras o métodos y medios de combate cibernéticos: la participación directa en las hostilidades 76

1. El principio de distinción en el ciberespacio 78

2. La participación directa en las hostilidades y los ciberataques 81

2.1. Requisitos 81

A. Umbral del daño 82

B. Causalidad directa 83

C. Nexo beligerante 85

2.2. Pérdida de la Protección 85

III. Conclusiones 87

CAPÍTULO 4

CIBERGUERRAS Y NIÑOS: NUEVOS DESAFÍOS PARA EL DERECHO INTERNACIONAL 91

Mª DEL ROSARIO CARMONA LUQUE

I. Introducción 92

II. Desafíos del derecho internacional humanitario ante los conflictos armados en el ciberespacio 93

III. La singular atención del derecho internacional al niño en el marco de los conflictos armados 99

Página

1. *Progresiva atención del Derecho Internacional al niño y su especial vulnerabilidad ante los conflictos armados* 99
2. *Reclutamiento y participación de niños en combate y respuesta del Derecho Internacional* 101

IV. **La ciberguerra y los niños: ¿nuevo escenario en busca de nuevas respuestas?** 108
1. *Posible incidencia de las nuevas tecnologías en el reclutamiento y participación de niños en conflictos armados* 108
2. *El Manual de Tallín: ¿una respuesta suficiente o una oportunidad perdida?* 112
3. *Propuestas de actuación desde el enfoque de los derechos del niño* 113

V. **Conclusiones** 115

PARTE II

CAPÍTULO 5

LA RESPUESTA DE LA UNIÓN EUROPEA A LOS CIBERATAQUES 119

LUCÍA MILLÁN MORO

I. **Introducción** 119

II. **Instrumentos de defensa de la Unión Europea frente a los ciberataques** 123
1. *El desarrollo normativo en la materia* 123
2. *Clasificación de los ciberataques según sus destinatarios* 126
2.1. Ciberataques dirigidos a la estructura institucional y orgánica de la UE 126
2.2. Ciberataques dirigidos a la UE en el ejercicio y desarrollo de sus competencias 129
2.3. Ciberataques dirigidos a los Estados miembros . 140
3. *El desarrollo orgánico de la Unión Europea para responder a los ciberataques* 142
3.1. Mecanismos de gestión de crisis 143
3.2. Mecanismos de cooperación 143

Página

3.3. Agentes 143
4. *La financiación económica de la investigación y la formación y la ayuda a la protección de los Estados miembros* 144
III. Conclusiones 146

CAPÍTULO 6
THE GLOBAL REGULATION OF CYBERSECURITY: A FRAGMENTATION OF ACTORS, DEFINITIONS AND NORMS 149
TATIANA NASCIMIENTO HEIM
RAMSES A. WESSEL

I. Introduction 149
II. The context: the governance of cybersecurity 152
III. A fragmentation of actors 156
IV. A fragmentation of definitions 159
1. *Defining cybersecurity* 159
2. *Defining cyber threat* 161
V. A fragmentation of norms 167
VI. Conclusion: from fragmentation to conso-lidation? 172

CAPÍTULO 7
DE CIBERATAQUES Y CIBERLEVIATANES: CARTOGRAFÍA DE LA "GOVERNANCE" EN EL PRISMA DEL DERECHO EUROPEO Y COMPARADO 175
ANTONIO LAZARI

I. Prolegómenos de la cuestión 176
II. La situación nacional interna al territorio de la Unión Europea 177
III. Normativas nacionales sobre ciberseguridad externas al territorio de la Unión Europea 180
1. *Panorama normativo en Estados Unidos de América* 180
2. *Panorama normativo en la República Popular China* 182
3. *Panorama normativo en la República Socialista de Vietnam* . 185

Página

4. *Panorama normativo en la Federación Rusa* 187
5. *Panorama normativo en la región MENA ("Middle Eastern and North African Countries")* 187

IV. Del análisis empírico a las consideraciones analíticas: los modelos de gobernanzas sobre ciberseguridad 189

V. Europa entre ciberleviatanes: las críticas neo-liberal y neo-marxista a los modelos de gobernanza actuales 192

1. *El ciberleviatán de Lassalle* 193
2. *La crítica al capitalismo de vigilancia de Zuboff* 195

VI. El pacto de Europa 197

VII. La normativa de la Unión Europea (UE) 198

1. *Rasgos del formante legislativo* 199
2. *European Governance* 200
3. *Ejemplos de "European Governance"* 200
   - 3.1. El nuevo Reglamento de ciberseguridad 200
   - 3.2. La propuesta de Reglamento sobre exportación de productos de doble uso 201
4. *Formante judicial* 201
5. *Diálogo judicial en el espacio jurídico europeo* 203

VIII. Epílogo 204

PARTE III

CAPÍTULO 8

INJERENCIA POLÍTICA EN EL CIBERESPACIO 209

MANUEL RICARDO TORRES SORIANO

I. El precedente soviético 210

II. Condicionantes de la injerencia política 213

III. Un nuevo punto de inflexión: la irrupción de la inteligencia artificial 215

1. *La democratización de la ofensiva* 215
2. *El colapso de la realidad* 216
3. *Dieta de datos* 219

Página

4. Hibridación entre el marketing digital y la propaganda política 221
IV. Conclusiones 222

CAPÍTULO 9
LA CIBERDELINCUENCIA COMO PROBLEMA ECONÓMICO GLOBAL: FACTORES DETERMINANTES Y CONSECUENCIAS 225
Mª TERESA ACEYTUNO PÉREZ

I. Introducción 225
II. Concepto, agentes y tipología de ciberdelincuencia 227
1. Concepto de ciberdelincuencia 227
2. Agentes 228
3. Tipología 230
III. Factores socioeconómicos determinantes de la ciberdelincuencia 232
IV. Impacto económico de la ciberdelincuencia 234
1. Dificultades de medición 235
2. Tipología de costes derivados de la ciberdelincuencia 236
3. Evolución de los costes de la ciberdelincuencia 236
V. Conclusiones 240

CAPÍTULO 10
LA ALIANZA ATLÁNTICA Y SU CIBERDEFENSA 243
GUILLEM COLOM PIELLA

I. Introducción 243
II. La ciberdefensa 1.0 246
III. La ciberdefensa 2.0 248
IV. La ciberdefensa 3.0 252
V. La ciberdefensa 4.0 259
VI. Conclusiones 264

Página

CAPÍTULO 11

INTERNATIONAL RELATIONS THEORY & CYBERSECURITY: THEMES AND DEBATES 267

JONATHAN PASS

I. **Introduction** 267
II. **Contrasting dominant ir paradigms** 269
1. *Realism & Neorealism* 269
2. *Liberalism & Neoliberalism* 271
3. *Social Constructivism & Post-Structuralism* 275
III. **Applying theories to cybersecurity** 279
1. *Realism & Neorealism* 279
2. *Liberalism & Neoliberalism* 284
3. *Critical Constructivism* 289

CAPÍTULO 12

INFLUENCERS AND FAKE NEWS ON TWITTER. DONALD TRUMP AS CASE STUDY 293

CONCHA PÉREZ CURIEL

I. **Introduction** 293
II. **Collateral effects of the twitter-trump influence on the media and fan communities** 294
III. **Research plan: methods, objectives and hypotheses** 296
1. *Quantitative/qualitative content worksheet* 298
IV. **Results analysis** 299
1. *Quantification and qualification indicators* 300
2. *Linguistic markers and discursivity* 304
V. **Conclusions** 306