Contenido

Listado de abreviaturas 17

Introducción 21

Parte I

Capítulo 1. El ciberespacio: un nuevo ámbito de la guerra 29

1. El ciberespacio: conceptualización 29
2. Características del ciberespacio 36
3. Principales vulnerabilidades del ciberespacio 38
   - 3.1. Vulnerabilidades del *Internet* 39
   - 3.2. Vulnerabilidades en el *hardware* y *software* 40
   - 3.3. El aumento de sistemas críticos en línea 40
4. Los ámbitos de la guerra 41
5. Incidentes cibernéticos 52

Capítulo 2. Estrategias y poder en el ciberespacio 67

1. Estrategias de ciberseguridad 67

1.1. ESTRATEGIA DE ESTONIA 68
1.2. ESTRATEGIA DE EE.UU. 69
1.3. ESTRATEGIA DE ALEMANIA 71
1.4. ESTRATEGIA DE ESPAÑA 72
1.5. ESTRATEGIA DE LA UNIÓN EUROPEA 74
1.6. ESTRATEGIA DE COLOMBIA 75
2. PODER E INSTITUCIONALIDAD MILITAR EN EL CIBERESPACIO 78
2.1. FUERZA AÉREA DE LOS EE.UU. 79
2.2. REAL FUERZA AÉREA DEL REINO UNIDO 80
2.3. FUERZA AÉREA COLOMBIANA 81

PARTE II

CAPÍTULO 3. RETOS DEL DERECHO INTERNACIONAL HUMANITARIO EN LOS CONFLICTOS ARMADOS EN EL CIBERESPACIO 83

1. CONFLICTO 85
1.1. ESCALAMIENTO DEL CONFLICTO 85
1.2. EL CONFLICTO EN EL CIBERESPACIO 87
1.3. DERECHO INTERNACIONAL HUMANITARIO O DE LOS CONFLICTOS ARMADOS 88
1.3.1. CONFLICTOS ARMADOS INTERNACIONALES 90
1.3.2. CONFLICTOS ARMADOS NO INTERNACIONALES 91

2. LEGALIDAD DEL CONFLICTO ARMADO Y LOS ATAQUES CIBERNÉTICOS.. 95

2.1. IUS AD BELLUM 95

2.1.1. ATAQUES CIBERNÉTICOS 97

2.1.2. CARACTERÍSTICAS DE LOS ATAQUES CIBERNÉTICOS 100

2.1.3. ATAQUES CIBERNÉTICOS COMO USO DE LA FUERZA 104

2.1.4. ALCANCE DE LA PROHIBICIÓN DEL USO DE LA FUERZA..... 114

2.1.5. REMEDIOS POR VIOLACIÓN 116

2.1.6. FORMAS DE USO DE LA FUERZA AUTORIZADO 117

2.1.7. ATAQUE CIBERNÉTICO COMO ATAQUE ARMADO 123

2.1.8. ATAQUE ARMADO Y LA AUTO-DEFENSA ANTICIPADA 126

2.1.9. LA AUTO-DEFENSA CONTRA ACTORES NO ESTATALES 133

2.1.10. LA ATRIBUCIÓN 136

2.1.11. La proporcionalidad, necesidad e inmediatez 138

2.2. IUS IN BELLUM 141

2.2.1. MÉTODOS Y MEDIOS DE USADOS EN UN ATAQUE CIBERNÉTICO..... 148

2.2.2. INTERVENCIÓN DE LAS FUERZAS ARMADAS 148

2.2.3. TERRITORIALIDAD Y SOBERANÍA 156

2.2.4. JURISDICCIÓN INTERNACIONAL 163

2.2.4.1. Jurisdicción legislativa 168

2.2.4.2. Jurisdicción judicial 171

2.2.4.3. Jurisdicción ejecutiva 173

2.2.5. ARMAS CIBERNÉTICAS: MÉTODOS Y MEDIOS DE GUERRA ... 176

2.2.5.1. Definición y estructura de un arma cibernética 176

2.2.5.1.1. Estructura de un arma cibernética . 178

2.2.5.2. Fundamento legal aplicable las armas cibernéticas 183

2.2.5.2.1. Principios generales 184

2.2.5.2.2. Regulaciones específicas 198

2.2.6. PARTICIPACIÓN EN LAS HOSTILIDADES 214

2.2.6.1. Combatientes 219

2.2.6.2. Sabotaje y espionaje 227

2.2.6.2.1. Espionaje 229

2.2.6.2.2. Sabotaje 236

2.2.6.3. Civiles 239

2.3. LA NEUTRALIDAD 245

2.3.1. BELIGERANTES 252

2.3.2. NEUTRALES 254

3. REGULACIÓN JURÍDICA SOBRE EL CIBERESPACIO 258

3.1. DERECHO INTERNACIONAL 259

3.1.1. DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS 259

3.1.2. LA ORGANIZACIÓN DE LAS NACIONES UNIDAS 270

3.1.3. UNESCO, LA SOCIEDAD DE INFORMACIÓN PARA TODOS ..273

3.1.4. ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES Y LA CARTA SOBRE DERECHOS EN INTERNET 274

3.1.5. LA OCDE Y LA ECONOMÍA DIGITAL 276

3.1.6. UNIÓN INTERNACIONAL DE COMUNICACIONES Y LA AGENDA DE SOLIDARIDAD DIGITAL 278

3.1.7. LA ORGANIZACIÓN DEL TRATADO DEL ATLÁNTICO NORTE 280

3.2. DERECHO REGIONAL 283

3.2.1. DERECHO REGIONAL EUROPEO 283

3.2.1.1. El Consejo de Europa 283

3.2.1.2. Convenio sobre la ciberdelincuencia 284

3.2.1.3. Protocolo adicional a la convención de Budapest del Consejo de Europa sobre persecución de los actos de racismo y xenofobia cometidos a través de internet 285

3.2.1.4. Convención de Lanzarote del año 2007 del Consejo de Europa sobre abuso y explotación sexual de los menores y pornografía infantil 286

3.2.1.5. La Unión Europea 287

3.2.1.5.1. Directiva 2011/93/UE sobre abuso, explotación sexual de los menores y pornografía infantil 287

3.2.1.5.2. Directiva 2013/40/UE sobre ataques a los sistemas de información 287

3.2.1.5.3. Decisión Marco 2008/919/JAI sobre lucha contra el terrorismo 288

3.2.1.5.4. La agenda digital para Europa 289

3.2.2. DERECHO REGIONAL AMERICANO 291

3.2.2.1. Organización de Estados Americanos 291

3.2.2.2. Derecho regional del ciberespacio aplicable a EE.UU. 294

3.2.2.3. Derecho regional aplicable a Colombia 296

3.3. LEGISLACIONES NACIONALES 297

3.3.1. LEGISLACIÓN DE ESPAÑA 297

3.3.2. LEGISLACIÓN DE EE.UU. 311

3.3.3. LEGISLACIÓN DE COLOMBIA 314

CAPÍTULO 4

PROPUESTAS DE SOLUCIÓN PARA LOS RETOS PLANTEADOS EN CONFLICTOS ARMADOS EN EL CIBERESPACIO

1. PROPUESTA ESTRATÉGICA DE MANEJO DE LA AMENAZA CIBERNÉTICA DESDE EL PUNTO DE VISTA DE SEGURIDAD INTERNACIONAL 322

1.1. ASPECTOS ESTRUCTURALES 325

1.2. ASPECTOS GEOPOLÍTICOS 328

1.3. ASPECTOS JURÍDICOS INTERNACIONALES Y LOCALES 335

2. PROPUESTA PARA LA ESPECIFICACIÓN DE UNA LEGISLACIÓN ADICIONAL 336

2.1. RESPONSABILIDAD PENAL PARA LOS ATAQUES CIBERNÉTICOS 339

2.2. PROTOCOLO ADICIONAL A LOS CONVENIOS DE GINEBRA PARA LOS CONFLICTOS ARMADOS INTERNACIONALES Y NO INTERNACIONALES EN EL CIBERESPACIO 352

2.3. PROTOCOLO ADICIONAL DE USO DE ARMAS CIBERNÉTICAS ADICIONAL A LA CONVENCIÓN DE ARMAS NO CONVENCIONALES 353

2.4. Examen jurídico para las armas cibernéticas 355

Conclusiones y reflexiones finales 359

Glosario de términos 365

Bibliografía 373

Legislación 383

Derecho Internacional Público 383

Derecho Regional 386

Legislación Nacional 386