EL CIBERDELITO. LA CONTRIBUCIÓN DE LAS ESTRATEGIAS DE SEGURIDAD A LA LUCHA CONTRA LA CIBERDELINCUENCIA: ARMAS JURÍDICAS CONTRA EL NUEVO ENEMIGO [1]

RAFAEL ÁLVAREZ OREJA-EGAÑA
Abogado
Doctorando en Seguridad de la Facultad de Derecho de la UNED

INTRODUCCIÓN

No resulta novedoso decir que las tecnologías o las formas de delincuencia aventajan al Derecho o las leyes. Esta vez los hechos parecen haber querido ganar la partida a la luz de la publicación del documento de máximo nivel de política estratégica, la Estrategia Española de Seguridad (EES).

El fenómeno de la delincuencia organizada en su dimensión de ciberdelincuencia se ha convertido en una de las amenazas al orden internacional y su lucha, en unos de los hándicaps a alcanzar dentro de las estrategias de lucha contra la cibercriminalidad y seguridad.

En la actualidad el escenario definido por la denominada "sociedad de la información" donde el substrato fundamental es la denominada 'información', el aumento del número de ordenadores, el incremento de la conectividad a Internet, son las principales variables para que los grupos de ciberdelincuencia persistan en la utilización de Internet como objetivo de sus actividades criminales.

La tecnología informática que se utiliza hoy en día es básicamente la misma en todo el mundo tanto para los países desarrollados como para los países subdesarrollados. La normalización y estandarización permite a los usuarios de todo el mundo acceder a los mismos servicios a través de Internet (2).

Hoy en día se estima que existen unos 542 millones de ordenadores en más de 250 países en cada continente (3). La distribución geográfica de internet se estima en 2.300

millones de usuarios que corresponde al 33 % de la población mundial (4).

Lo que nos lleva a pensar que internet no es sólo una simple red, sino un conjunto de ordenadores con una gran variedad de formas de conexión, ya sea individual o colectiva a través de organizaciones ilegales.

Pueden llegar a cualquier punto sin tener en cuenta fronteras físicas o geográficas independientemente de la franja horaria en la que nos encontremos, en cualquier momento y desde cualquier lugar.

Las cifras (5) reflejan con certeza que la actividad delictiva llevada acabo por la ciberdelincuencia se haya convertido en el nuevo enemigo a combatir en todos sus ámbitos por los miembros de la comunidad internacional.

Al igual que las referencias apuntan no sólo que gracias a las tecnologías los grupos de delincuencia han encontrado una buena forma de lucrarse, sino que existe una evolución en la forma de utilización de internet.

La ciberdelincuencia ha convertido la triada compuesta por la confidencialidad, integridad y disponibilidad de la información, así como, la integridad y disponibilidad de los sistemas que los sustenta en sus intereses tanto tácticos como estratégicos.

En este sentido las estrategias de la lucha contra la ciberdelincuencia han hecho hincapié dentro de sus políticas en la necesidad de armonizar y homogeneizar estas conductas.

Los contenidos introducen este tipo de conductas a través del instrumento armonizador del Convenio sobre la Ciberdelincuencia del Consejo de Europa (6).

El Convenio trata de que se penalicen en los Derechos Nacionales de los países ratificantes, entre otras, esta nueva categoría de delitos incluidos en el Capítulo II Título I. Los denominados *"Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos".* Concretamente expresando:

En su Artículo dos el *"Acceso Ilícito".*

En su Artículo tres la *"Interceptación ilícita".*

En su Artículo cuatro la *"Interferencia en los datos".*

En su Artículo cinco la *"Interferencia en el sistema".*

En su Artículo seis el *"Abuso de los dispositivos".*

El panorama estratégico de seguridad de los diferentes Estados (7) ha hecho un avance positivo en esta cuestión aportando dentro de sus políticas la integración de medidas legales. En este sentido han hecho de la legislación parte integrante de las estrategias de seguridad. Contribución que ha favorecido el fortalecimiento de las medidas de lucha contra la cibercriminalidad. Concretamente han llegando a incluir la pertinencia dentro de sus recomendaciones para la adhesión al propio Convenio (8).

La actual Estrategia Española de Seguridad (9) (en adelante EES) no es ajena ha esa integración. Han fortalecido con "armas jurídicas" el efecto disuasorio que obliga tener todo tratamiento de la seguridad cuyo fundamento se asemeja a los criterios de la lucha contra la cibercriminalidad.

Algunas de las aportaciones que han reforzado estas "armas jurídicas" son las siguientes:

Reconoce la existencia de un nuevo ámbito o entorno (10) específico denominado ciberespacio donde la fortaleza de su seguridad está en la mejora de la legislación (11).

Reconoce una nueva amenaza al ciberespacio denominada ciberamenaza. La seguridad del ciberespacio puede estar comprometida por ataques ilícitos denominados ciberataques (12). Esta nueva forma representa la evolución de la actividad delictiva en forma de "ataques informáticos" o acciones mecanizadas (13) cuyo objeto son los principios de la confidencialidad, integridad y disponibilidad de los sistemas de información.

Impulsar a nivel internacional la criminalización de las conductas que en forma de amenaza o ataque alteran interrumpiendo, interceptando, modificando el flujo de información (14).

Refuerza de nuevas competencias a la Fiscalía Especial incluyendo el crimen organizado de especial relevancia como es en su caso, su dimensión de la ciberdelincuencia (15).

El conjunto de aportaciones intensifica el rol disuasivo de la Justicia Penal que necesita el aumento delictivo y su compleja composición.

Refiriéndose al diagnóstico de la utilidad desde el punto de vista delictivo. Necesarios para propugnar ciertos cambios de mentalidad que lleven a reconstruir el poder disuasivo de la justicia dentro del ciberespacio.

El objeto del trabajo es esbozar entre líneas dentro del documento de máximo nivel estratégico español, el tratamiento de las políticas dirigidas a configurar las "armas jurídicas", todas ellas, hacer valer el rol disuasorio de la Justicia.

La "Teoría de la Disuasión" (16) (Becker, 1968) incorpora en su análisis la política de seguridad y justicia como instrumentos determinantes de la lucha contra la delincuencia.

Supone que el criminal comete un delito sólo si la utilidad esperada de una actividad ilegal excede a la utilidad que obtendría si empleara ese tiempo y esos recursos en una actividad legal.

Esa utilidad esperada de cometer un crimen va a depender de los beneficios esperados y los costos derivados de delinquir. Entre estos últimos se encuentra la probabilidad de ser arrestado, la probabilidad de ser condenado en caso de ser atrapado y la severidad de las penas en caso de ser condenado.

La nueva forma delictiva en combinación con el espacio geográfico donde se desarrolla, orientada a un reforzamiento de aspectos de la utilidad penal como marco ciberdisuasorio, da paso al siguiente desarrollo:

En un primer lugar se analizará el reconocimiento que se hace por primera vez del ciberespacio como nuevo espacio geográfico cuyo terreno es un flujo interminable de información en forma de bits. El reconocimiento como nuevo ámbito o espacio geográfico le convierte en el nuevo espacio geopolítico a considerar.

Las teorías geopolíticas han servido para ordenar la influencia del espacio geográfico sobre los Estados, sus políticas de seguridad y la necesidad de construcción de normas de convivencia basadas en el control territorial.

Algunas de las partes geopolíticas de un Estado son las comunicaciones y las fronteras. Las comunicaciones son los conductos que unen las diversas zonas del territorio entre sí y con otros Estados. Otorgan contextura al Estado, posibilitando la circulación de diversos medios económicos, políticos, militares y culturales para lograr la unidad necesaria. Las fronteras son las líneas que delimitan el ámbito de la soberanía de dos Estados. Su solidez o debilitamiento revelan la salud de un Estado. En las fronteras se produce el enfrentamiento y resistencia de las presiones de las soberanías de los países colindantes. Actualmente son delimitadas a través de tratados internacionales.

La existencia de un nuevo factor geográfico sin fronteras ha venido a significar la necesidad de tratar un nuevo escenario geopolítico. Las teorías geopolíticas deben formar parte de las políticas emprendidas en las estrategias de seguridad con el objetivo de asegurar el control jurisdiccional sobre el territorio.

En este sentido las conductas delictivas en un entorno tipificadas como tal son también consideradas conductas delictivas en el ciberespacio. Por lo que los poderes a través de la Justicia tienen el deber y el derecho de poder hacer cumplir la ley de los malos usos de la red.

El espacio geográfico del ciberespacio con la ayuda de la identificación valdría fácilmente para minimizar los beneficios que han encontrado los grupos de ciberdelincuencia gracias a sus características. La reducción del anonimato ayudaría a aumentar la posibilidad de ser identificado con su efecto directo sobre la utilidad criminal.

Es importante para estos intereses tomar las influencias geopolíticas que sirvieron para controlar los espacios antecesores sobre el espacio geográfico a través de medidas que sean, entre otras, capaces de reducir el anonimato.

En un segundo apartado se desarrolla el marco teórico que, con ayuda de un instrumento armonizador, propone las estrategias de seguridad. La homogeneización penal que refuerza la utilidad del rol disuasivo de la Justicia al establecer una nueva categoría de delitos denominados "*Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos".*

Los aspectos técnicos de las acciones ilícitas de estos delitos son los expresados en las actuales EES como el acceso ilegal al conjunto o una parte de los sistemas de información, la intromisión, interrupción, obstaculiza-

ción o daño sobre un sistema de información, o la intromisión ilegal en sus datos.

Para este apartado la articulación de esta descripción plantea la tipificación de la actividad delictiva cuando la confidencialidad, integridad y disponibilidad son el objetivo consumado de las pretensiones de los grupos de ciberdelincuencia.

Estos principios son los atributos objeto de protección de la Seguridad de la Información. Los principios de la seguridad de la información son la confidencialidad, integridad y disponibilidad. Son delitos contra esta categoría si estan dirigidos al menos contra uno de esos tres principios jurídicos.

En un tercer lugar el intento de abordar en las estrategias de seguridad el nuevo enemigo con “armas jurídicas”.

El intento de abordar la evolución habida en las formas de considerar al nuevo enemigo, hacen necesario que las políticas se adecuen al nuevo escenario estratégico. Abordándolas con aspectos legales como parte integrante de los factores disuasorios que obligan las estrategias de seguridad.

Durante todos los tiempos se han proyectado modelos estratégicos a través de los cuales las fuerzas políticas, militares, diplomáticas y económicas han tratado de garantizar los intereses nacionales de los Estados.

Los cambios ocurridos en las amenazas al orden internacional, la existencia de un nuevo factor geográfico denominado ciberespacio y el nuevo modelo de sociedad liderada por las tecnologías de la información, han alterado las estrategias a tenor de que las amenazas dejan de tener un carácter puramente militar.

En las actuales estrategias de seguridad el marco ciberdisuasorio se centra en el refuerzo de la tipificación homogeneizada de las acciones ilícitas contra el medio (el flujo de información como objetivo de los ataques) y en el fortalecimiento de los mecanismos técnicos que ayuden a los fundamentos de la utilidad.

En el apartado final se realizará una aproximación al grado de contribución que ha realizado España en la integración (17) dentro de nuestro ordenamiento a tenor de lo establecido en las EES.

Para concluir el breve trabajo quiero dejar abierto el estudio de la actividad criminal cuando el objeto jurídico lesionado o puesto en peligro es la Seguridad de la Información (ataques contra la confidencialidad, integridad y disponibilidad de la información o sistemas informáticos) por la conducta de la ciberdelincuencia (sujeto activo).

Si partimos de un nuevo terreno geográfico dominado por el ciberespacio cuyas amenazas fundamentadas en ataques informáticos han hecho evolucionar el marco ciberdisuasorio. Las corrientes de estudio deben ir encaminadas a completar un sistema de responsabilidad de usuario que persiga fundamentalmente: La identificación del usuario; la trazabilidad, integridad y legibilidad de los impulsos electrónicos. Por ultimo, la retención de esos impulsos como evidencia para que en los procesos judiciales se conviertan en prueba.

Esta vez la tecnología contrastada con todos estos avances armonizadores pudiera jugar a favor de la lucha contra la ciberdelincuencia.

EL NUEVO ESCENARIO GEOPOLÍTICO: EL CIBERESPACIO COMO NUEVO ESPACIO GEOGRÁFICO

La influencia de los factores geográficos (18) sobre la conducción política, las relaciones del hombre con el territorio y el dominio de los Estados han estado siempre presentes. El reconocimiento controlado, seguro y libre del entorno ha sido necesario para la distribución del poder de los Estados y sus desarrollos.

La geopolítica (19) representa un instrumento para definir y enfocar estrategias políticas según los intereses en el espacio geográfico (20) o las representaciones que tienen los Estados, pueblos o grupos sociales dentro de ese escenario.

El conjunto de políticas que han integrado los modelos estratégicos ha sabido adaptarse a los intereses y situaciones geopolíticas (21) de cada momento.

Por ejemplo, al terminar la Segunda Guerra Mundial uno de los componentes de las estrategias de seguridad llevada a cabo fue la integración de políticas de disuasión.

El propósito era llegar a todos los ámbitos conocidos de la tierra, el mar y el aire. De esta forma quedaba garantizado el efecto disuasorio por toda la dispersión geográfica.

Las estrategias disuasorias desarrollaban sus métodos tácticos particulares para llegar a todos los ámbitos o terrenos conocidos hasta el momento.

La disuasión nuclear se hacía llegar a través de los vectores de la denominada "triada nuclear". En el ámbito terrestre a través del despliegue sobre el terreno de sus misiles estratégicos intercontinentales. En el ámbito marítimo através de sus submarinos nucleares. Por último, en el ámbito aéreo, con sus bombarderos estratégicos.

El fin del periodo de Guerra Fría marca un hito importante en la evolución de la historia del pensamiento y del planteamiento estratégico de muchos aspectos geopolíticos, no sólo en un nuevo diseño del orden mundial, sino además en la configuración de los contenidos de las estrategias de seguridad.

Las estrategias de seguridad habidas culminan con la noción clásica de enemigo (22). Dan paso a un nuevo periodo estratégico donde se reconocen, por un lado, un nuevo ámbito que devalúa la importancia del espacio territorial a favor de un espacio virtual. Por otro, lleva a considerar nuevas amenazas (23) que hacen entender una nueva forma a la Seguridad.

La evolución de las principales teorías geopolíticas (24) ha tenido como denominador común la visión del poder mundial através de los dominios de los poderes terrestre, naval, aéreo y espacial.

Según han ido apareciendo nuevos dominios han ido vinculando su control con la capacidad de poder ostentar el dominio de su espacio. Así sucedió en su momento con la aparición de una "una cuarta dimensión", es decir, la dimensión espacial, estrechamente vinculada a la capacidad tecnológica del Estado (25).

La EES, establece la actual situación geográfica que junto a los ámbitos clásicos terrestre, marítimo, aéreo y espacial incluye la existencia de un nuevo ámbito estratégico no antes reconocido con tal claridad como es el denominado ciberespacio.

El ciberespacio es el espacio virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas web, foros, servicios de Internet y otras redes. Creado por el ser humano, es un entorno singular para la seguridad, sin fronteras geográficas, anónimo, asimétrico, que puede ser utilizado de forma casi clandestina y sin necesidad de desplazamientos. Es mucho más que la Red, pues incluye también dispositivos como los teléfonos móviles, la televisión terrestre y las comunicaciones por satélite.

En palabras del responsable de uno de los organismos encargados en la mejora de la seguridad en este ámbito, el Director del Centro Criptológico Nacional (26), pone de relieve un nuevo modelo de sociedad con la ayuda de las tecnologías *"El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas"* (27).

Principalmente este entorno sin fronteras geográficas liderado por el anonimato cuyo uso pudiera ser totalmente clandestino, ha convertido que el ciberespacio sea el nuevo y "distinto" ámbito de oportunidad criminal.

Las ventajas que ofrecen este espacio geográfico a la actividad criminal son actualmente conocidas, entre otras:

Facilidad de acceso y mantenimiento. Las tecnologías de la información y comunicaciones utilizadas es básicamente la misma en todo el mundo (28).

Inexistencia de fronteras naturales que hace que existan diferentes enfoques legislativos y en algunos casos escasa o diferente regulación.

Escaso control gubernamental para mecanismos de control de investigación.

Anonimato para diferenciar y probar el tipo de acción y, en definitiva, identificar a los atacantes.

Rapidez en el intercambio de información y comodidad para la planificación y control de sus operaciones.

Alcance global gracias a la fuerza multiplicadora de la Red.

Bajo coste de la realización de ataque.

El ciberespacio ha creado nuevas oportunidades globales para los Estados y sus gentes en los diferentes puntos del espectro del desarrollo económico, político, administrativo y cultural. En contraposición, esa morfografía del ciberespacio, cuyos caracteres de tiempo y espacio (29) con el carácter transnacional (30), hacen bastante dificultosa la atribución, favoreciendo el anonimato.

Los fundamentos geopolíticos en virtud del desarrollo tecnológico que componen mayormente el quinto ámbito, debe buscar sobre todo, mecanismos con capacidad de poder ejercer su jurisdicción en todo sus terrenos al igual que ocurrió con los otros ámbitos.

La morfología del ciberespacio debe planear crear y sostener un entorno en el que las conductas responsables no desvirtúen el estado de derecho del ciberespacio, teniendo en cuenta la realidad internacional y transnacional de producción de esta forma de delincuencia.

En este sentido las conductas delictivas en el entorno son también consideradas conductas delictivas en el ciberespacio. Por lo que los poderes a través de la Justicia tienen el deber y el derecho de hacer cumplir la ley.

El ciberespacio necesita desarrollar un sistema de monitorización que sea capaz de identificar las intrusiones, localizar la fuente del ataque con una trazabilidad tan exhaustiva que pueda soportar opciones diplomáticas, militares, políticas y legales, además debe ser capaz de hacer todo esto en milisegundos. (McConnell, 2010).

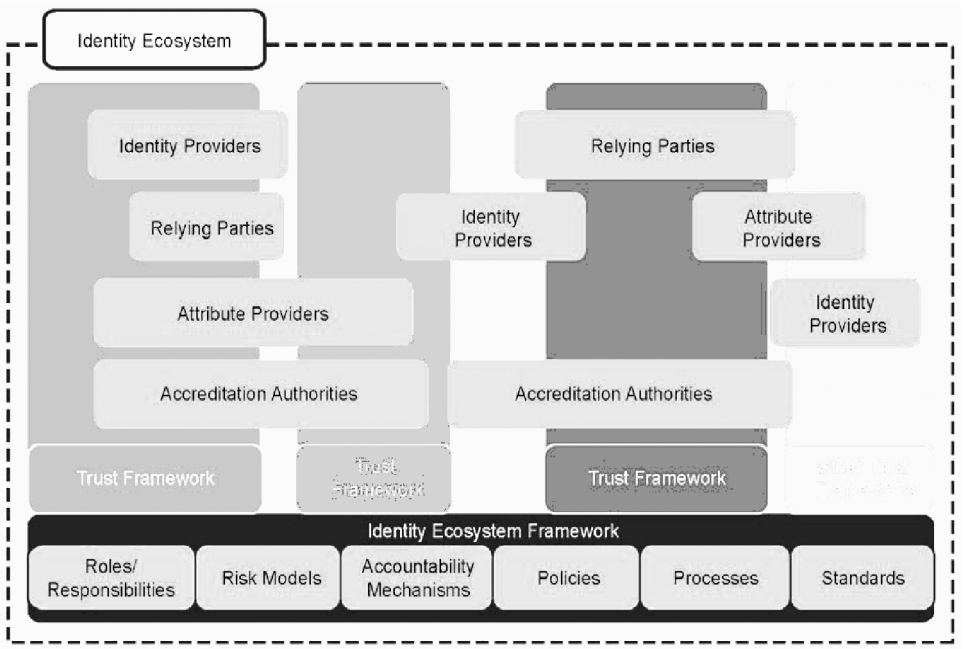
El ciberespacio es el quinto ámbito que hay que proteger además de la tierra, el mar, el aire y el espacio.

El control del ciberespacio pasa por que las estrategias de seguridad se orienten ante la capacidad de poder reducir el anonimato. Sin duda hay bastante campo para efectuar mejoras en este campo.

El establecimiento de determinadas reglas de juego que reduzcan la posibilidad de reducir el anonimato en este espacio sin fronteras tendría un enorme efecto sobre la ciberdelincuencia. Es necesario un reconocimiento controlado que haga seguro y libre el entorno.

Actualmente se esta trabajando en este sentido de establecer una única identidad digital en internet a través de estrategias de seguridad.

Concretamente, Estados Unidos esta inmersa en un proyecto (31) para la creación de un ecosistema de identificación para entrar en Internet (ciberespacio) con el que se solucionarían muchos problemas de seguridad en la red.



Identity Ecosystem Framework. Fuente: National Strategy for Trusted Identities in cyberspace.

UNA NUEVA FORMA DELICTIVA: LOS DELITOS CONTRA LA SEGURIDAD DE LA INFORMACIÓN

La protección y la seguridad de la información han cobrado ahora una importancia crítica, hasta el punto que constituye un requisito previo para el crecimiento del comercio electrónico, el funcionamiento de la economía, el bienestar y la seguridad.

La seguridad de los sistemas de información suscita cada vez más preocupación, hasta el punto de que a través de las estrategias de seguridad se requieran esfuerzos para que los ataques contra sus sistemas sean sancionados penalmente.

Las EES establecen dentro de sus prioridades trabajar en la homogeneización de la legislación penal de los países miembros de la Unión Europea en aspectos como el acceso ilegal al conjunto o una parte de un sistema de información, la intromisión, interrupción, obstaculización o daño sobre un sistema de información o la intromisión ilegal en sus datos.

La característica de estas prioridades representa penalmente la fisonomía tecnica de las amenazas contra el flujo de información.

En este contexto flujo (32) se entiende como secuencia de intercambio e interacción (33) determinados, repetitivos y programables entre posiciones físicamente inconexas (JEDSABEL, 2005).

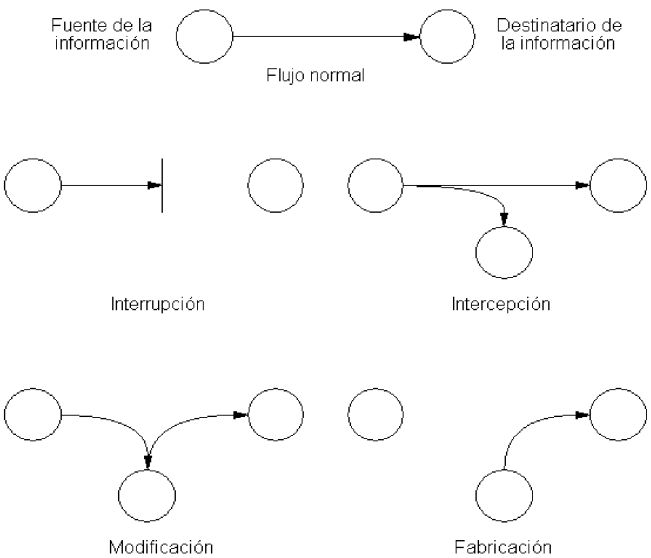
La definición de informática (34) es el conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento automatizado de la información por medio de ordenadores.

El ordenador es la maquina destinada a procesar datos. El termino “informática”, es una palabra que se deriva de “información” unida a “automatización”, nos da como resultado el concepto de proceso automatizado de la información.

Una vez que la información ha sido procesada y se muestra su resultado de modo inteligible en la unidad mas pequeña de información, en computación se le denomina bit (dígitos 0 y 1), pasan a formar parte del flujo de información (35).

La materialización de la amenaza, de tal forma, que pudiera interceptar, interrumpir o modificar el flujo de información es considerada un ataque contra un sistema informático.

Es decir, se convierte en una violación contra la seguridad de la información en alguno de sus atributos de confidencialidad, integridad o disponibilidad (36). En el ámbito penal es más apropiado hablar de ataque como acción consumada que hablar de amenaza. La amenaza penalmente consiste en el anuncio de un mal futuro ilícito mediante cualquier medio de comunicación (37).



Fuente: Instituto de la Seguridad de la Información del Consejo Superior de Investigaciones Científicas.

La interrupción se produce cuando un recurso del sistema es destruido o se vuelve no disponible. La consumación de esta acción deliberada será un ataque contra la disponibilidad.

La interceptación se produce cuando un servicio o entidad no autorizada consigue acceso a un recurso. En estos casos estaríamos ante un ataque contra la confidencialidad.

La modificación se produce cuando una entidad o servicio no autorizado, no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad.

En estos términos es importante la identificación de las palabras "acceso", "uso" y "autorización" ya que el uso de alguna de ellas implica un uso desapropiado de las otras en el entorno de los sistemas informáticos.

"Acceso" y hacer "uso", no es el mismo concepto cuando se estudian desde el punto de vista de usuario o de un intruso (atacante). Cuando un usuario tiene acceso autorizado quiere decir que tiene autorizado el uso de un recurso o servicio.

Cuando un atacante tiene "acceso desautorizado" está haciendo uso desautorizado del sistema y si lo hace del sistema lo hace de la información que el sustenta.

Cuando un atacante hace "uso desautorizado" de un sistema implica que el acceso pudo ser autorizado o no autorizado.

Por lo que un ataque es un intento de "acceso" (con éxito o sin el), o "uso" desautorizado de un recurso, sea satisfactorio o no.

El intento de "acceso" reiterado o la degradación de la capacidad de un sistema para prestar servicios y proporcionar recursos o información a los usuarios se traducen en ataques contra la disponibilidad.

El uso desautorizado de un recurso, servicio o información nos lleva a ataques contra la integridad o confidencialidad.

En el ámbito de la Organización Internacional de Estandarización ISO (38), establece en su normativa ISO/IEC 27000 (39) la definición de Seguridad de la información como la preservación de la confidencialidad, integridad y disponibilidad de la información.

La "integridad" (inglés: Integrity) es el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad, característica de salvaguardar la exactitud y completitud de los activos.

La "confidencialidad" (inglés: Confidenciality) es el acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]:" característica, propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

La "disponibilidad" (inglés: Availability) es el acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Otros organismos establecen la Seguridad de los Sistemas de Información (40) en la protección de los sistemas de información respecto al acceso no autorizado o modificación de la información en el almacenamiento, proceso y tránsito y contra la denegación de servicio para los usuarios autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y contrarrestar dichas amenazas.

De todo este conjunto de definiciones de normativas y cuerpos legales, tanto de organismos de carácter público como privado, se deriva la existencia de tres conceptos o principios básicos importantes y dignos de protección respecto a los sistemas de Información así como de los sistemas que los soportan.

Estos son la Confidencialidad, Integridad y Disponibilidad así como de integridad y disponibilidad respectivamente.

En el ámbito de Defensa se hace hincapié en lo recogido en la Orden Ministerial 76/2002, de 18 de abril en la que se establece de manera explicita los conceptos de confidencialidad, integridad y disponibilidad bajo su ámbito recogido en la Orden Ministerial 76/2006, de 19 de Mayo, por la que se aprueba la política de Seguridad de la Información del Ministerio de Defensa.

La política de Seguridad de la Información del Ministerio de Defensa tiene por objeto alcanzar la protección adecuada, proporcionada y razonable de la información del Ministerio de Defensa, mediante la preservación de sus requisitos básicos de seguridad: confidencialidad, integridad y disponibilidad.

El termino elegido como *confidencialidad* lo define como requisito básico de seguridad que garantiza que solo las personas, entidades o procesos autorizados pueden acceder a la información.

La Integridad como requisito básico de seguridad que garantiza que la información no pueda ser o no ha sido modificada o alterada por personas, entidades o procesos no autorizados

Así como la *disponibilidad* como requisito básico de seguridad que garantiza que se pueda acceder a la información y a los recursos o servicios que la manejan conforme a las especificaciones de los mismos.

La guía de la Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC) del Centro Criptológico Nacional (41) define Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC) como la protección de la información almacenada, procesada o transmitida, por Sistemas de las Tecnologías de la Información y las Comunicaciones (Sistemas), mediante la aplicación de las medidas necesarias que aseguren o garanticen la confidencialidad, integridad y disponibilidad de la información y la integridad y disponibilidad de los propios Sistemas.

En las dimensiones internacionales del ciberdelito la respuesta jurídica ante los "ataques informáticos" los considera delitos cuando están dirigidos al menos contra uno de los tres principios jurídicos de confidencialidad, integridad y disponibilidad (42).

Por todo ello podemos considerar una nueva categoría denominada "Delitos contra la Seguridad de la Información".

EL NUEVO MARCO DISUASORIO: DE LA DISUASIÓN CONVENCIONAL A LA CIBERDISUASIÓN

Después de un periodo de estrategias de contención, durante la guerra fría (43), la rivalidad entre las dos grandes superpotencias, Estados Unidos de América (EE.UU.) y la Unión Soviética (URSS), daba forma a la configuración del modelo conceptual de seguridad así como los métodos para hacer efectivas sus pretensiones a través de sus estrategias disuasorias.

El argumento a favor de la configuración de ese modelo pasaba por los efectos que pudiera producir la amenaza real a la seguridad. Los efectos que producían eran gracias a la tecnología nuclear y su potencial destructivo. La destrucción mutua asegurada, levantaba enormes inhibiciones en el empleo de ese tipo de armas y es en lo que vino a denominarse la disuasión nuclear (44).

El elemento principal que surgió de esas estrategias, mas allá de la operatividad de las armas nucleares, estaba en el efecto psicológico que producía en el adversario la posible utilización de sus arsenales. Es decir, el riesgo a la destrucción mutua era el elemento determinante de la disuasión.

Una vez terminado el periodo de la guerra fría, la táctica operativa de la disuasión nuclear que constituía un mecanismo de protección absoluta, pasó a un segundo plano. La configuración del nuevo escenario de las amenazas ha llevado consigo a la necesidad de realizar cambios en la percepción de las estrategias de seguridad.

Sobre todo, en articular métodos disuasorios capaces de hacer efectiva las nuevas estrategias a tenor de que las amenazas dejan de tener un carácter puramente militar.

La perdida de la noción clásica de enemigo que acompaño con el fin de la guerra fría ha provocado un profundo cambio en el modelo tradicional de seguridad.

Los argumentos a su favor se basan en tres pilares básicos (45):

Las amenazas actuales no respetan las fronteras nacionales, están relacionadas entre sí, y deben encararse tanto en los planos mundial y regional como en el plano nacional.

Ningún Estado, por más poderoso que sea, puede hacerse invulnerable, por si solo, a las amenazas actuales.

Y no se puede suponer que todo Estado podrá o querrá siempre cumplir su deber de proteger a su propia población y no causar daño a sus vecinos.

Estos pilares llevaron a configurar un nuevo planteamiento de la seguridad a favor del concepto de seguridad colectiva (46).

En la actualidad en el ámbito de protección de la seguridad internacional, hay seis grupos

de amenazas que deben preocupar al mundo de hoy (47):

Las amenazas económicas y sociales, como la pobreza, las enfermedades infecciosas y la degradación ambiental.

Los conflictos entre Estados.

Los conflictos internos, como la guerra civil, el genocidio y otras atrocidades en gran escala.

Las armas nucleares, radiológicas, químicas y biológicas.

El terrorismo.

La delincuencia organizada transnacional.

En diciembre de 2003, la Unión Europea adopto la Estrategia Europea de Seguridad (48) cuyo contenido se ocupaba de la dimensión exterior de la seguridad de Europa. En este contexto se ponía de relieve como una de las principales amenazas a la delincuencia organizada. En su alcance, esta amenaza interna se convertía en un objetivo primordial para su seguridad.

La situación de la amenaza preveía en ese periodo que ninguna de las nuevas amenazas es meramente militar, ni puede ajustarse su protección únicamente con medios militares en virtud del medio donde transcurren. Las amenazas tienen un carácter dinámico por el lugar donde se desarrollan.

Más tarde la respuesta de la Unión Europea (49) a la lucha contra la delincuencia organizada se adapta a la complejidad del fenómeno y contempla las nuevas dimensiones de delincuencia organizada como es la ciberdelincuencia (50).

En febrero de 2010 (51), el Consejo Europeo completo la Estrategia Europea de Seguridad adoptando la Estrategia de Seguridad Interior. En ella convertía la prevención y la lucha contra las amenazas comunes en un factor clave para garantizar una calidad de vida en la sociedad europea. Las amenazas comunes que incluye la Estrategia de Seguridad Interior son la delincuencia organizada y su dimensión de la ciberdelincuencia.

La EES vincula la nueva amenaza con la ciberamenaza (52) vinculando su materialización con los ciberataques. Los ciberataques son una amenaza donde incluye a los grupos de delincuencia organizada como posibles agresores. Identifica la importancia de los sistemas de información para la estabilidad y prosperidad económica de nuestro país con la seguridad del ciberespacio. Establece la mejora de su seguridad sobre el fortalecimiento de dos parámetros fundamentales: Fortalecer la legislación y reforzar la capacidad de resistencia y recuperación.

Las estrategias disuasorias convencionales obligan a dejar paso a un nuevo concepto de disuasión. La combinación de la nueva amenaza y el ciberespacio hacen necesario establecer un marco ciberdisuasorio que sea capaz de conseguir o al menos disminuir las pretensiones de la delincuencia en su versión de ciberdelincuencia.

El ciberespacio es algo virtual, difiriendo completamente de lo que rodea al mundo físico. Las redes digitales tienen inherente un efecto sin límites, sin fronteras, con una infinita fragilidad y abstracción en medir el daño de los potenciales atacantes. Pueden estar a tu lado sin darse uno cuenta. Ellos mismos pueden desconocen en muchas ocasiones el daño potencial que pueden producir con su posible ataque. Las herramientas que utilizan son las mismas para un delincuente o grupo de ellos como para un estudiante juvenil o herramientas de trabajo domestico. La automatización no hace necesario que detrás de cada ataque tenga haber una persona física.

Por todo ello el marco ciberdisuasorio, a tenor del carácter extremamente técnico, debe ser capaz de fortalecer la legislación y reforzar la capacidad de resistencia de recuperación que sirvan como medidas ciberdisuasorias.

La definición de este marco ciberdisuasorio (53) en relación con la EES pasa por incluir los siguientes factores:

La noción o sensación por parte de los agresores de la capacidad de penalización o castigo.

La noción o sensación de frustración del ataque a través de la resistencia o recuperación de los sistemas.

La noción o sensación de que la acción realizada tiene capacidad de respuesta y persecución inmediata en toda su amplitud.

En el ámbito de la doctrina estratégica disuasoria, “ser disuadido, es ser llevado a preferir

la situación que resultara de la inacción a aquella que resultaría de la acción en el caso que esta desencadenara las consecuencias previstas, es decir, la ejecución de las amenazas explícita o implícitamente proferidas. La acción (ataque) es más reducida cuanto mas completa es la disuasión (54)".

LA INTEGRACIÓN DE LAS PRIORIDADES ESTRATÉGICAS DE SEGURIDAD EN EL MARCO PENAL ESPAÑOL

A medida que las sociedades dependen cada vez más de las tecnologías, se hace necesario utilizar medios jurídicos y prácticos eficaces para gestionar los riesgos asociados a las infraestructuras de información.

Así lo han previsto las actuales EES al incluir dentro de sus líneas estratégicas la homogeneización de la legislación penal de los Estados miembros de la Unión Europea. En estos momentos existe mucho trabajo avanzado en estos términos, no solo a nivel internacional, sino a nivel nacional.

A finales del año 2000 (55), la necesidad de un proceso de integración para la creación de una sociedad de la información más segura mediante la mejora de las infraestructuras de información y la lucha contra las actividades delictivas cuando el objeto son esas propias infraestructuras.

En el ámbito de la Unión Europea, se inicia a través del Parlamento Europeo un llamamiento para que se establezcan definiciones comúnmente aceptables de este tipo de delincuencia y se aproximen las legislaciones, en especial en el ámbito penal.

La Cumbre de Tempere del Consejo Europeo celebrada en octubre de 1999, en apoyo a la utilización de medios jurídicos como parte de integrante de las estrategias de lucha de esta forma de delincuencia, introdujo esfuerzos orientados para acordar definiciones, tipificaciones y sanciones comunes.

En ese momento, el Consejo de la Unión Europea adopto posiciones comunes respecto el Convenio del Consejo de Europa sobre la delincuencia en el ciberespacio, adoptando aspectos de su contenido como parte de la estrategia de la Unión contra la delincuencia denominada como de alta tecnología.

A su vez la Comisión se proponía promover y fomentar las acciones europeas tendentes a la seguridad de la información. Diferenciando entre los delitos informáticos específicos y los delitos tradicionales perpetrados con ayuda de la informática.

El trabajo del Consejo de Europa relativo al Convenio sobre la delincuencia en el ciberespacio estuvo orientado en cuatro categorías de delitos. Concretamente, en el sentido más estricto que describe y tipifica las conductas, cuando las infraestructuras de información son el objetivo. Son los Delitos contra la confidencialidad, la integridad y disponibilidad de los sistemas y datos informáticos.

El Convenio sobre la Ciberdelincuencia del Consejo de Europa hecho en Budapest el 23 de noviembre de 2001 representa una aproximación a escala internacional que introduce los instrumentos jurídicos necesarios para armonizar dentro de los derechos nacionales de la UE en este tipo de delincuencia.

El Convenio, en su Capítulo II, Título I, expone la necesidad para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos y la tipificación de esos actos.

La ratificación de los convenios internacionales hace de ellos la incorporación vinculante al orden jurídico interno de los países. Su jerarquía en la escala normativa nacional depende de lo establecido en la respectiva constitución respecto a los tratados ratificados. En nuestro territorio nacional, a excepción de sus reservas, los convenios tienen rango supra legal quedando sin efecto las disposiciones legales contrarias tanto si son anteriores como posteriores a la ratificación.

España firmo el Convenio por esas mismas fechas y lo ratifico con el instrumento de ratificación el 17 de Septiembre de 2010.

En este sentido, más tarde nace la Decisión marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques de los que son objeto los sistemas de información. La decisión completa y refuerza la lucha contra la ciberdelincuencia a través de la aproximación de las normas penales que reprimen los ataques contra la seguridad de la información.

A este efecto, la presente decisión marco

propone una aproximación de los sistemas de Derecho penal, concretamente a lo que respecta al acceso o intromisión ilícito a un sistema de información y el perjuicio a la integridad de un sistema o datos.

En Derecho comunitario, una "decisión" es un acto de carácter normativo obligatorio en todos sus elementos para los destinatarios que en ella se designan.

En combinación, especialmente en el ámbito de la armonización jurídica europea que exige la Decisión Marco y la ratificación del Convenio, se incardinan las conductas penales en la reforma del Código Penal con la ley Orgánica 5/2010, de 22 de Junio.

El actual código penal recoge lo relativo a los daños, donde quedarían incluidas las consistentes en dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno. Por otro, referido al descubrimiento y revelación de secretos, donde estaría comprendido el acceso sin autorización vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema o en parte del mismo.

España en confirmación con las necesidades estratégicas de refuerzo de nuevas competencias a la Fiscalía Especial. Apoya a finales del 2011 la creación del organismo especializado para la lucha contra las manifestaciones criminales cometidas directamente contra los sistemas informáticos a través de la instrucción 2/2011 de la Fiscalía General del Estado sobre la criminalidad informática.

La instrucción 2/2011 determina, entre otros, el catalogo inicial a los que se extiende el marco competencial de la criminalidad informática. En ese primer catalogo incluye los delitos de contra la seguridad de la información.

Los delitos cuando el objeto de la actividad delictiva son los propios sistemas informáticos o las tecnologías de la información y las comunicaciones (TIC) son lo siguientes:

– Delitos de daños, sabotaje informático y ataques de denegación de servicios previstos y penados en el artículo 264 y concordantes del Código Penal.
– Delitos de acceso sin autorización a datos, programas o sistemas informáticos previstos y penados en el artículo 197.3 del Código Penal.
– Delitos de descubrimiento y revelación de secretos del artículo 197 del Código Penal cometidos a través de las TIC o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos.
– Delitos de descubrimiento y revelación de secretos de empresa previstos y penados en el artículo 278 del Código Penal cometidos a través de las TIC o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos ó electrónicos.
– Delitos contra los servicios de radiodifusión e interactivos previstos y penados en el artículo 286 del Código Penal.

CONCLUSIÓN

En el ámbito naval, la piratería es una práctica organizada con propósitos de robar, capturar la nave o secuestrar a sus integrantes, atacando en aguas internacionales, lugares no sometidos a jurisdicción de ningún Estado o, en su momento, no eran capaz de llegar para hacer cumplir su soberanía a través de su potencial naval de intramar. En definitiva, es una forma fácil de lucrarse ilícitamente aprovechando las carencias del espacio naval.

En el ámbito aéreo, en el Convenio de Aviación Civil Internacional, expresa el reconocimiento de la soberanía del Estado, plena y exclusiva, "en el espacio aéreo situado sobre su territorio". En su contenido establecen que la plena protección y la seguridad de la aviación civil internacional deben ser garantizadas. Aquella aeronave, objeto volante, real o aparente que no puede ser identificado y cuyo origen es desconocido, se convierte en un objeto volador no identificado.

El Estado no sólo se encuentra facultado para sancionar las violaciones de las normas de la naturaleza comentada que ocurran dentro de su territorio, sino también fuera de él, cuando las aeronaves que lleven el distintivo de su nacionalidad infringen las disposiciones indicadas en el territorio de otros países.

En el reglamento (56) por el que se establecen los requisitos en materia de identificación de aeronaves para la vigilancia del cielo único europeo define "identificación de una aeronave" como grupo de letras o de cifras, o combinación de ambas, que es idéntico o que forma un código equivalente al indicativo de la aeronave que debe utilizarse en las comunicaciones aire-tierra y que se emplea para identificar la aeronave en las comunicaciones tierra-tierra de los servicios de tránsito aéreo.

En el ámbito terrestre las matriculas de los vehículos es el instrumento indicativo de identificación.

A través de los tiempos, la consideración de nuevos ámbitos ha llevado consigo problemáticas semejantes con su coetáneo ciberespacio. Por un lado, la falta de identificación o sometimiento de jurisdicción, ha favorecido la actividad delictiva. Llámese piratería naval, robo de vehículos o de matricula o piratería informática o ciberdelincuencia. Por otro, la identificación ha estado presente en la solución de la reducción de anonimato como solución a muchos de los problemas que plantea el uso del medio.

Las aportaciones de las Estrategias de Seguridad indican la posibilidad de realizar reformas estructurales en internet orientadas a la identificación. Al menos así lo necesitan la legislación penal que integra la seguridad y protección del ciberespacio.

En los primeros momentos de creación de internet se plantearon dos corrientes: Los que abogaban por la necesidad de prevenir y sancionar los malos usos en la red y los que defienden que internet debe estar libre de intervencionismos por chocar directamente contra el derecho a la intimidad y de la libertad de expresión (57).

Si las actuales estrategias definen por primera vez un nuevo terreno cuya seguridad efectiva pasa por buscar la aplicación de la jurisdicción penal a través de todo su territorio, para que el rol de la Justicia Penal sea práctica y proporcione seguridad, se debería dotar de un sistema de asignación de responsabilidad cuyas metas abarquen: la identificación del usuario, la trazabilidad, integridad y legibilidad de la información así como la retención de la evidencia ante los tribunales (58). Sino, todo lo trabajado en la aproximación de la legislación penal en materia de ataques contra los sistemas de información y los datos informáticos será en vano.

La efectividad del marco disuasorio va a depender de la reducción del anonimato a través de la identificación que proporcione la probabilidad de ser arrestado, la posibilidad de ser condenado en caso de ser atrapado y la severidad de las penas en caso de ser condenado.

BIBLIOGRAFIA

IVAN INFANTAS BARBACHAN. *"Visión Geográfica del Ciberespacio"*. Magister en Geografía. Instituto Geográfico Agustín Codazzi.

AGUSTINA SANLLEHI, JOSE. *"La arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual"*. Profesor Doctor de Criminología y Derecho Penal. Universitat Internacional de Catalunya. ISSN 1988-7949. 2009.

STEIM SCHJOLBERG, Chief Judge. *"The History of Global Harmonization on Cybercrime Legislation - The road to Geneva"* December, 2008.

FERNANDO MIRO LLINARES. *"La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen"*. Profesor Titular de Derecho Penal. Universidad Miguel Hernandez de Elche (2011) ISSN 1695-0194.

XII CONGRESO DE LAS NACIONES UNIDAS sobre Prevención del Delito y Justicia Penal Salvador (Brasil), Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético, 12 a 19 de abril de 2010.

MARILÚZ GUTIÉRREZ FRANCÉS. Profesora titular de derecho penal Universidad de Salamanca. Reflexiones sobre la ciberdelincuencia hoy (en torno a la ley penal en el espacio virtual).

MARCELO A. RIQUERT. CRISIS PENAL: Política Criminal Globalización y Derecho Penal. Ediciones EDIAR. Argentina.2007.

THOMAS J. MOWBRAY, ADVISOR: DR. KEES LEUNE Solution Architecture for Cyber Deterrence. Accepted: April 12, 2010.

CYBER-DETERRENCE (April 2010 v2.1) Forthcoming in Law, Policy and Technology: Cyberterorrism, Information Warfare, Digital and Internet mobilization (IGI Global 2010). K. A. Taipale Founder.

PAUL ROSENZWEIG National Research Council Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy. The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence. July 2010.

A FRAMEWORK FOR THINKING ABOUT CYBER CONFLICT AND CYBER DETERRENCE, WITH POSSIBLE DECLARATORY POLICIES FOR THESE DOMAINS. Center for International Strategy, Technology, and Policy The Sam Nunn School of International Affairs Georgia Institute of Technology, Atlanta, Georgia.

PALOMA LLANEZA. *"La reforma 2010 del Código Penal"*. Revista SIC. Seguridad informática y comunicaciones. Febrero 2011.

PALOMA LLANEZA. *"De las evidencias a las pruebas"*. Revista SIC. Seguridad informática y comunicaciones. Febrero 2009.

ADAN DEL RIO, CARMEN. *"La persecución y sanción de los delitos informáticos"*. Eguzkilore Número 20. San Sebastián, diciembre 2006.

NOTAS

(1) *"Armas jurídicas contra el nuevo enemigo"*. Título utilizado en el artículo publicado en El PAÍS con fecha 22/10/2010. Autor: Manuel Cancio Meliá. Catedrático de Derecho Penal de la Universidad Autónoma de Madrid referente a los cambios introducidos en el Código Penal vigente en relación al terrorismo internacional. El actual trabajo utiliza la denominación de "armas jurídicas" por ser el marco legal el denominador común en las estrategias de la lucha contra la cibercriminalidad y de seguridad. Las "armas jurídicas" proporcionan en las actuales estrategias de

seguridad, el rol disuasivo, gracias a la integración del Sistema de Justicia Penal dentro de sus contenidos.

(2) *"El ciberdelito: Guía para los países en Desarrollo"*. Recursos jurídicos contra el ciberdelito. División de Aplicaciones TIC y Ciberseguridad. Departamento de Políticas y Estrategias. Unión Internacional de Telecomunicaciones. Abril 2009.

(3) Fuente 2009: Internet Software Consortium's Internet Domain Survey; www.isc.org.

(4) Fuente: Internet World Stat - www.internetworldstats.com. December 2011.

(5) El informe de Symantec sobre ciberdelincuencia (2011) muestra las cifras relacionadas con la ciberdelincuencia. Dentro de esta cifra se encuentran las pérdidas directas provocadas a las víctimas por un total de 274 mil millones de dólares (tanto en dinero como en tiempo) y los costos que significa intentar controlar la delincuencia informática, cifra que llega a los 114 mil millones de dólares. A nivel mundial, unas 430 millones de personas han sufrido algún tipo de ataque o ciberdelito durante el período analizado del año 2011, lo que coloca a este tipo de delito por encima del mercado negro de marihuana, cocaína y heroína en lo que se refiere a costos para combatirlo. http://es.norton.com/cybercrimereport/promoç

(6) Convenio sobre la Ciberdelincuencia hecho en Budapest el 23 de Noviembre de 2001 del Consejo de Europa es el principal instrumento internacional que cubre las áreas necesarias que requiere la lucha contra la ciberdelincuencia (derecho penal sustantivo, derecho procesal y cooperación internacional).

(7) Ver.: National Strategies & Policies http://www.ccdcoe.org/328.html.

(8) Estados Unidos de America (USA): International Strategy for Cyberspace of United state of America. Prosperity, Security, and Openness in a Networked World. Mayo 2011. Pag. 19, 20.

Alemania: Cyber Security Strategy for Germany (February 2011) Page 4, 11.

Francia: Information systems defence and security - France's strategy (February 2011) Page 4, 8.

(9) Estrategia Española de Seguridad. (EES) "Una Responsabilidad de todos". Gobierno de España. Madrid 2011.

(10) Ídem 10, Pág. 41.

(11) Ídem 10, Págs. 13, 66.

(12) Ídem 10, Págs. 13, 18.

(13) Eloy Velasco Núñez: DELITOS COMETIDOS a través de INTERNET. Cuestiones Procesales. Editorial LA LEY. Grupo Wolters Kluver. Termino utilizado para identificar el ataque informático.

(14) Ídem 10, Pág. 69.

(15) Ídem 10, Pág. 54.

(16) Principio esbozado dentro de la Teoría de la Disuasión por Gary Becker y que le valió posteriormente el Premio Nobel de Economía.

(17) La integración tiene su antecedente directo en el desarrollo de la tesis doctoral del programa de investigación del Ciberdelito llevada a cabo por el Doctorando D. Rafael Álvarez Oreja-Egaña del Doctorado en Seguridad de la Facultad de Derecho de la Universidad Nacional a Distancia (UNED). Constituye el objeto de la línea de investigación el estudio pluridisciplinar de la actividad criminal llevada a cabo por la amenaza de la delincuencia organizada en su dimensión de ciberdelincuencia, cuando sus objetivos son la información o los sistemas que los sustentan.

Como eje central de la investigación, es analizar en qué medida los "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos", se configuran dentro de los cuerpos normativos nacionales de los países integrantes de la Escuela Europea de Policía (CEPOL) y son ratificantes del Convenio sobre la Ciberdelincuencia, concretamente, respecto a los delitos cuando al Capítulo II Título I titulados.

(18) Gustavo Rosales Ariza. Director Instituto de Estudios Geoestratégicos y Asunto políticos (IEGAP) Universidad Militar Nueva Granada. *Ensayos "Geopolítica y Geoestratégica liderazgo y poder"*. Gustavo Rosales Ariza. http://www.iegap-unimilitar.edu.co. Los aspectos geográficos han sido determinantes en la evolución y cultura para el desarrollo de los pueblos. *"... los sumerios, cultura fundamental de nuestra civilización, se establecieron sobre la confluencia de los ríos Tigris y Eufrates; los antiguos egipcios a lo largo del río Nilo; los primitivos chinos sobre el río Amarillo y las culturas precursoras de los actuales hindúes en los ríos Indo y Ganges. Más tarde los persas se extendieron sobre el Asia Menor buscando su acceso al Mediterráneo y los romanos, posteriormente, hicieron de este mar su "Mare Nostrum" con lo cual privilegiaron la permanencia de su imperio. Siglos más tarde los europeos preocupados porque el dominio turco sobre la "Ruta de la Seda" les impedía comercializar con el Extremo Oriente se dieron a la tarea de hallar otras rutas; entonces los portugueses circunnavegaron la desconocida África y Colón al servicio de Castilla y Aragón se encontró con el Nuevo Mundo..."*

(19) Jorge E. Atencio. *"Qué es la Geopolítica"*, Ediciones Pleamar, Buenos Aires, 1965.

Friedrich Ratzel, precursor de la geopolítica. (1844-1904): "La Geopolítica es la ciencia que establece que las características y condiciones geográficas y, muy especialmente, los grandes espacios, desempeñan un papel decisivo en la vida de los Estados, y que el individuo y la sociedad humana dependen del suelo en que viven, estando su destino determinado por las leyes de la Geografía. Proporcionando al conductor político el sentido geográfico necesario para gobernar".

(20) Ver www.cybergeography.org - Atlas de internet con datos comparativos.

(21) *Técnicas del proyecto Geopolítico*. Programa Administración publica territorial. Álvaro Alegría Guerrero. Escuela Superior de Administración Pública. Pags. 6-26.

(22) Documentos de Seguridad y Defensa, *"Hacia una estrategia de seguridad Nacional para España"*, Centro Superior de Estudios de la Defensa Nacional (CESEDEN), Ministerio de Defensa, Febrero 2009. Pags. 15-17.

(23) Estrategia Española de Seguridad. Una responsabilidad de todos. Ed. 2011. Gobierno de España. Ministerio de la Presidencia. Pags. 10-13. La Estrategia Española de Seguridad identifica las amenazas y las líneas de acción para hacerle frente. La ciberamenaza. "Cada vez una mayor parte de nuestra actividad se desarrolla en el ciberespacio, donde las amenazas pueden ocasionar graves daños e incluso podrían paralizar la actividad de un país..."

(24) Víctor Giudice Baca. Profesor principal de la Facultad de Ciencias Económicas de la Universidad Nacional Mayor de San Marcos. Gestión en el Tercer Milenio, Rev. de Investigación de la Facultad de Ciencias Administrativas, UNMSM (Vol. 8, Nº 15, Lima, Julio 2005). Pág. 20.

Ídem 11. Págs. 19-23.

En ambas reseñas expresa la Teoría del poder Naval de Alfred Mahan (1840-1914) basada en los principios del poder marítimo. Por otro, la teoría del poder Terrestre de Hartford Mac Kínder (1905). Por ultimo la teoría del poder aéreo de Alexander Seversky (1950) que consideraba que la existencia de un poder aéreo permitiría someter a los dos anteriores.

(25) *Ídem 11*. Pág. 22.

(26) Fuente: https://www.ccn-cert.cni.es. El principal objetivo del CCN es contribuir a la mejora del nivel de seguridad de los sistemas de información de las tres administraciones públicas existentes en España (general, autonómica y local). "Su misión es convertirse en el centro de alerta nacional que coopere y ayude a todas las administraciones públicas a responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir y afrontar de forma activa las nuevas amenazas a las que hoy en día están expuestas".

(27) Gobierno de España, Centro Criptologico Nacional (CCN-CERT), Ministerio de Presidencia. Prologo Guías Serie 800 del Esquema Nacional de Seguridad. 2010. Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

(28) *Ídem 2*, Pag. 15.

(29) FERNANDO MIRO LLINARES. Profesor Titular de Derecho Penal. Universidad Miguel Hernández de Elche "*La oportunidad criminal en el ciberespacio"*. Revista Electrónica de Ciencia Penal y Criminología ISSN 1695- 0194. 13 de Julio de 2011. Caracteres del ciberespacio. Pags. 5-10. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Tiempo y espacio son coordenadas que las nuevas actividades conocen bien para la perpetración de sus actividades.

(29) *Ídem 4*. Pag 13. Incluye los aspectos delictivos de la ciberamenaza

(30) El ciberespacio favorece en toda su amplitud el carácter transnacional del ciberdelito. La actividad criminal: a) Se comete en más de un Estado; b) Se comete dentro de un solo Estado, pero una parte sustancial de su preparación, planificación, dirección o control se realiza en otro Estado; c) Se comete dentro de un solo Estado, pero entraña la participación de un grupo delictivo organizado que realiza actividades delictivas

en más de un Estado; o d) Se comete en un solo Estado, pero tiene efectos sustanciales en otro Estado.

(31) Ver: *National Strategy for Trusted Identities in Cyberspace*.

(32) JEDSABEL ORDÓÑEZ, Adriana. Tesis Doctoral. "Los nuevos flujos de la información, la ciudadanía y la sociedad" Pontificia Universidad Javeriana. Facultad de Estudios Políticos y Relaciones Internacionales. Bogotá 2005. Págs. 79-85.

(33) En un ámbito técnico estas interacciones son un circuito de impulsos electrónicos cuyo procesamiento tiene un carácter informático (dígitos 0 y 1).

(34) Diccionario de la Real Academia de la Lengua. Vigésimo segunda edición 2011.

(35)

(36) Departamento de Tratamiento de la Información y Codificación del Instituto de Seguridad de la Información del Consejo Superior de Investigaciones Científicas de España. http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html.

(37) Se regula en los artículos 169 y siguientes del actual Código penal vigente.

(38) Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares. La ISO es una red de los institutos de normas nacionales de 163 países, sobre la base de un miembro por país que coordina el sistema. La Organización Internacional de Normalización (ISO) está compuesta por delegaciones gubernamentales y no gubernamentales subdivididos en una serie de subcomités encargados de desarrollar las guías que contribuirán al mejoramiento del ámbito normalizado: ambiental, seguridad, alimentario etc.

(39) ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organización Internacional para la Standarization) e IEC (International Electrotécnica Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044. La ISO 27002 es el Código de buenas prácticas en gestión de la seguridad de la información.

(40) INFOSEC Glossary 2000.

(41) Guía de seguridad CCN-STIC-800 Esquema Nacional de Seguridad. Centro Criptológico Nacional. Organismo.

(42) *Ídem 2,* pág. 21.

(43) La Segunda Guerra Mundial termino en el año 1945. El periodo posterior denominado Guerra fría va desde su término hasta el fin de la URSS. El final de la URSS ocurrió en 1989 con la caída del muro de Berlín y el golpe de estado ocurrido el 1989. El cuño de este período se debe a las tensiones geopolíticas entre las potencias resultantes de la SGM, Estados Unidos de América (EE.UU.) y URSS (Unión de Repúblicas Socialista Soviéticas). La Guerra Fría determino en buena medida la política mundial de los 45 años siguientes.

(44) Desde el punto de vista psicológico, la disuasión basada en armas nucleares entre otros elementos, levanta enormes inhibiciones contra el empleo de las propias armas, motivada por la mutua destrucción asegurada. *LA DISUASIÓN EN LA ÁREA DE LA PROLIFERACIÓN NUCLEAR*. The Wall street Journal. Henry A. Kissinger, George Shultz,W Perry y Sam Nunn.

(45) www.un.org/secureworld - Un mundo más seguro: la responsabilidad que compartimos. Informe del Grupo de Alto Nivel sobre amenazas, los desafíos y el cambio. Plan para hacer frente a las amenazas siglo XXI. A /59/565 Asamblea General. Parte I Hacia un nuevo consenso en materia de seguridad (2005).

(46) Se entiende como Seguridad Colectiva como cualquier suceso o proceso que cause muertes en gran escala o una reducción masiva en las oportunidades de vida y que socave el papel del Estado como unidad básica del sistema internacional que constituye una amenaza a la seguridad internacional. La seguridad colectiva, además de englobar diferentes políticas (económicas, de defensa, exterior, social) de varias naciones.

Pone de relieve que el propósito de la seguridad frente a este grupo de amenazas es imposible de alcanzar de forma individual. "Todos contra el enemigo al compartir intereses comunes". La manera de hacer efectiva la seguridad colectiva frente a la amenaza de la delincuencia organizada en su dimensión de ciberdelincuencia pasa por el establecimiento de convenios internacionales e instrumentos jurídicos armonizados.

(47) Informe del Grupo de Alto Nivel sobre amenazas, desafíos y el cambio de las. Titulado "Un mundo más seguro: la responsabilidad que compartíos", Naciones Unidas 2005. Pág. 12.

(48) Estrategia Europea de Seguridad. Bruselas 12 de Diciembre de 2003. "Una Europa Segura en un mundo Mejor". Pag. 4.

(49) europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/index_es.htm

(50) La ciberdelincuencia representa una amenaza global, técnica transfronteriza y anónima. Se configura como una de las nuevas amenazas al orden mundial. Estrategia de Seguridad Interior de la Unión Europea Marzo 2010. Pág. 14.

(51) Estrategia de Seguridad Interior. 2010. Bajo la presidencia semestral española fue aprobada por el Consejo de Europa de los días 25 y 26 de marzo de 2010. "Hacia un modelo europeo de seguridad".

(52) ATENCION EES pag 13 y 65.

(53) Para la descripción de esta aproximación del estudio de nuevas formas ciberdisuasoria es el expuesto en el Documento K.A. Taipale. "Cyber - deterrence". Forthcoming in Law, Policy and Technology: Cyber terrorism, Information Warfare, Digital an Internet Immobilization. Stilwell Center for Advanced Studies in Science and Technology Policy Senior Fellow. World Policy Institute, USA. (IGI Global 2010). Pags. 28-42.

(54) Raymond Aron.

(55) Comunicación de la comisión al consejo, al parlamento Europeo, al comité económico y social y al comité de las regiones. "Creación de una sociedad de la información mas segura mediante la mejora de la seguridad de las infraestructuras de información y lucha contra los delitos informáticos." Comisión de las comunidades europeas. Bruselas 26/1/2001. COM (2000) final.

(56) REGLAMENTO DE EJECUCIÓN (UE) N.º 1206/2011 DE LA COMISIÓN de 22 de noviembre de 2011 por el que se establecen los requisitos en materia de identificación de aeronaves para la vigilancia del cielo único europeo.

(57) INTERNATIONAL E_JOURNAL OF CRIMINAL SCIENCIES, Prof. Dr. Jose Agustina Sanllehi. Profesor de Criminología y Derecho Penal. Universitat Internacional de Catalunya. *"La arquitectura digital de internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual"*, Artículo 4 Número 3 2009 ISSN: 1988-749, págs. 4-5.

(58) *Cybercrime*. Digital Cops in Networked Environment. The information Society Project at Yale Law School. Designing Accountable Online Policing. Nimrod Kozlovski. Pag. 125.