UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

LA CONFIGURACION DE UNA POLITICA DE SEGURIDAD Y DEFENSA EN EL CIBERESPACIO PARA LA UNION EUROPEA: EL MANUAL DE TALLIN

T E S I S

PARA OBTENER EL TÍTULO DE

LICENCIADA EN RELACIONES INTERNACIONALES

P R E S E N T A

BRISA ANAYATZIN ENRIQUEZ DIAZ

DIRECTOR DE TESIS

DR. JESUS GALLEGOSC OLVERA

CIUDAD UNIVERSITARIA, CDMX, agosto 2018

Índice

Línea del Tiempo

Mapas

Tablas

IMÁGENES

Introducción

> *La sociedad no determina la tecnología, sí puede sofocar su desarrollo, sobre todo por medio del estado. O, de forma alternativa y sobre todo mediante la intervención estatal, puede embarcarse en un proceso acelerado de modernización tecnológica, capaz de cambiar el destino de las economías, la potencia militar y el bienestar social.*
>
> *Manuel Castells*

La Guerra Fría representó, para el mundo, un tiempo de tensión y cambios. Los avances tecnológicos estaban a la orden del día y dirigidos a la innovación tecnológica para la guerra. Terminado este período de la historia fueron muchos los descubrimientos científicos en el mundo y de espacios que el hombre ha buscado dominar. El espacio exterior y el ciberespacio fueron los nuevos lugares de encuentro en disputa por los países, solo que el segundo tardó más en captar la visión de los gobiernos y su importancia.

El ciberespacio representó, en un primer momento, una revolución tecnológica que cambiaría la forma de comunicación del mundo moderno. Tanto por la transformación en las relaciones entre los individuos como en las relaciones estatales y comerciales donde la interconexión del mundo ha sido inevitable. El ciberespacio se ha transformado en un medio que elimina las fronteras de los países y unificado más al mundo pero esto no siempre es algo positivo.

En los últimos años, el ciberespacio se ha convertido en un nuevo escenario de conflicto crecidamente complejo debido a la evolución constante que en sí mismo representa dejando vulnerables a los actores que participan en él. La digitalización de los Estados (cuyas instituciones comienzan a funcionar a través del ciberespacio) pueden verse como un beneficio a futuro que convertirá a los países en más desarrollados pero también los convierte en un blanco fácil de ataques dentro de este nuevo espacio. La conciencia respecto a los peligros que representa la era digital reafirma la necesidad de una estrategia que atienda los nuevos retos que se presentan.

Sin embargo, ha provocado una dependencia de los diferentes sectores donde cualquier falla podría suponer una amenaza en materia de seguridad de cualquier tipo (sanitaria, energética, económica, etc.). Por ello, es necesario destacar la necesidad de crear acciones que otorguen a este nuevo escenario una estrategia en seguridad y defensa para evitar una verdadera catástrofe.

Es el 27 de abril de 2007, cuando se hace una demostración de las capacidades que un Estado puede tener dentro del ciberespacio. Tras varias diferencias por la discriminación étnica en Estonia a la comunidad rusa y con el pretexto de que se retiró una estatua erigida en la época soviética en homenaje a los soldados que lucharon contra la invasión alemana en la Segunda Guerra Mundial, nombrada como "El soldado de Bronce", se provoca el descontento de Rusia y sus comunidades en ese país.

Este hecho influyó para que días después el sistema informático de Estonia fuese atacado y dejará al país desconectado del mundo. Hay que destacar que Estonia era un país conectado al ciberespacio en un 97% y el ciberataque provocó el colapso de sus redes de comunicación, bancarias, etc. Esto produjo una crisis social y dejó en claro la falta de mecanismos preventivos que ayudaran a combatir este tipo de sucesos. Aunque la Unión Europea fue la primera en apoyar, tampoco contaba con una estrategia que ayudase a Estonia haciendo repensar varios temas primordiales para la seguridad de un Estado.

A partir de este momento, no solo Estonia se vería retado y comprometido con los temas de ciberseguridad que acogieron a su nación, sino que la Unión Europea replantearía las iniciativas que a lo largo de su historia ha comenzado a constituir. Por ende, se debe estudiar como el Manual de Tallin constituye un elemento importante para la construcción de la ciberseguridad de la Unión Europea. Y lo que podría significar en un futuro ya que el Manual de Tallin deja a la luz aquellos temas que no se han tomado en cuenta, dejando la posibilidad de crear una política de seguridad y defensa mejor estructurada.

El Manual es la base de esta investigación pues constituye un elemento importante para la construcción de la ciberseguridad tanto en la Unión Europea como en Estonia. El Manual de Tallin saca a la luz aquellos temas que no se han tomado en cuenta, dejando la posibilidad de crear una política

de seguridad y defensa mejor estructurada para la comunidad europea y para la sociedad internacional. El Manual es una base que permite ver los problemas primordiales que competen al mundo en la cuestión del ciberespacio y con ello conformar una política que prevenga cualquier incidente de este tipo.

Así, la hipótesis central de esta investigación parte de que el Manual de Tallin representa un primer acercamiento a las medidas que un Estado puede tomar con respecto a un ciberataque y por ello se constituye como la base para la creación de una Política de Seguridad y Defensa en el ciberespacio para la Unión Europea. En este sentido, permite la apertura de un debate para la creación de una legislación internacional sobre el ciberespacio a partir de la aplicación de estas medidas y sus efectos posibles en la política de seguridad y defensa.

La investigación se abordará a partir de un criterio deductivo y sistemático. En lo deductivo se enfocará en analizar los postulados del Manual de Tallin para comprobar su validez y las posibilidades que tienen de ser aplicados como iniciativas en la creación de una política de seguridad y defensa en el ciberespacio para la Unión Europea. En cuanto a lo sistemático, se partirá del análisis de la estrategia de protección en el ciberespacio que ha construido la Unión Europea.

Esta investigación tendrá por objetivo comprender los conceptos que construyen al ciberespacio a partir de la injerencia del Estado en este espacio. Así como de describir las decisiones conjuntas que se han tomado en la Unión Europea para la protección del ciberespacio. Y, analizar la influencia del Manual de Tallin en la construcción de una política de seguridad y defensa en la Unión Europea. Se guiará por 3 capítulos que desglosaran la concepción del ciberespacio, las iniciativas de ciberseguridad de la UE y los postulados del Manual de Tallin que pueden ser utilizados para la construcción de una Política de Seguridad y Defensa en la Unión Europea y sus efectos a nivel internacional.

En el capítulo 1, Nociones sobre el ciberespacio, planteará las bases para la investigación a partir de la conceptualización de diferentes aspectos que tendrán relación con el Manual. En una primera instancia, se retoman los conceptos de ciberespacio e internet, la diferencia de los mismos y cómo ha

cambiado su definición a lo largo de los años pues aún no son consensadas a un nivel internacional y muchas veces varía según el campo de estudio. Además de hacer una pequeña comparación con la obra de William Gibson (Neuromancer) que puso de moda el termino de ciberespacio.

Este capítulo también aborda dos conceptos importantes que da la base para considerar al ciberespacio un espacio: el espacio geográfico y la cibergeografía. Aunque realmente el segundo es un estudio sobre el ciberespacio y su posible mapeo, es a partir del espacio geográfico que se constituye la idea de considerar al ciberespacio un nuevo espacio de interacción no físico. Pues su influencia llega a diferentes niveles como es el económico, político, y hasta jurídico. A partir de esta idea se estudian las amenazas posibles dentro del ciberespacio a partir de las amenazas físicas tradicionales y asimétricas.

Más adelante, se toman los conceptos básicos y que influyen en la construcción tanto de políticas de ciberseguridad en el mundo como del Manual de Tallin. Estos conceptos son: Infraestructuras críticas, ciberataque, ciberseguridad, ciberguerra, ciberdefensa y ciberestrategia. En lo que se refiere a Infraestructura crítica se hace un primer señalamiento a la Infraestructura física que compone al ciberespacio y después de las Infraestructuras Críticas de un Estado, cuáles son y la forma en que pueden repercutir si se ven amenazadas. En cuanto a los ciberataques, se definen y se describen los tipos de ciberataques existentes.

La ciberguerra, parte de la idea de la militarización del ciberespacio. Como es que se ha desarrollado en diferentes países, como en Estados Unidos, ciberejércitos que tienen un entrenamiento similar al de un ejército físico. A partir de aquí se busca comprender la idea de la ciberguerra, las similitudes con la guerra física y los posibles ataques que podrían considerarse como armas de ciberguerra y la necesidad de comprender este nuevo aspecto de la guerra a partir de sus componentes como es el anonimato, la inexistencia de fronteras y los virus informáticos.

Sobre ciberseguridad, ciberdefensa y ciberestrategia, se abordan a partir de sus definiciones y en conjunto porque tienen una relación estrecha al momento de plantear alguna de ellas. No existe ciberdefesa sino se plantea una ciberseguridad y para ello hay que crear una ciberestrategia que permita la

prevención de cualquier ciberataque. Se describen los tipos de amenazas y el efecto que una de ellas puede tener a nivel internacional.

Como última cuestión, se menciona la Teoría de la Globalización en un mundo interconectado. A partir de aquí, se busca enfatizar la relación entre el ciberespacio y la globalización. Como es que la llegada de Internet se compagina con la globalización y a partir de esta unión comienza un crecimiento en ambos aspectos en donde el mundo es transformado. Con esta idea se retoman los posibles escenarios del investigado Sean Gallagher y se comenta la posibilidad de estos en un escenario futuro real.

El capítulo 2, La Unión Europea y los desafíos del ciberespacio, es un capítulo más sencillo de explicar pero el más extenso. Este capítulo se enfoca en la historia de la Unión Europea respecto a sus políticas relacionadas con las telecomunicaciones y en su tiempo con el ciberespacio. Desde sus primeras políticas con el Libro Verde de las Telecomunicaciones en 1989 hasta su Estrategia de Ciberseguridad en 2016.

Este recorrido histórico es importante en la investigación pues denota los temas que la Unión Europea ha dado prioridad al momento de crear políticas que regulen las actividades en su ciberespacio. De este tema se pueden sacar varias impresiones, una de ellas es la prioridad de la UE por considerar los aspectos económicos sobre los políticos. Además de que siempre se ha mantenido muy al margen sobre los desarrollos en políticas que direcciones sus intenciones en las redes sociales. En especial, su enfrentamiento constante entre los intereses de sus miembros, las políticas nacionales de cada uno y los intereses de sus miembros externos.

El capítulo 3, Manual de Tallin y la configuración de una política de seguridad y defensa en la Unión Europea, es el eje central de la investigación. Este capítulo se divide en dos partes, la primera hace el recuento de los hechos acontecidos en Estonia en 2007, las fallas, las debilidades y las soluciones que se tomaron para poder enfrentar una desconexión total. Asimismo, se evalúan las posibilidades del por qué se eligió a Estonia como blanco de este hecho y las posiciones políticas de Rusia.

La segunda parte del capítulo busca evaluar al mismo Manual de Tallin y todas las alternativas para la protección de las redes europeas que surgieron. Se mencionan los mecanismos que Estonia y sus socios tomaron para evitar

que se volviese a presentar un escenario similar. Y como estos mecanismos desembocaron en la necesidad de los debates para la creación de un Manual que pudiera regular las situaciones de guerra en el ciberespacio.

Esta segunda parte desarrolla la composición del Manual, los elementos prioritarios de mayor crítica, además de enlistar los retos y las oportunidades que presenta el Manual para Estonia, la comunidad europea y la sociedad internacional. Tras el listado, se busca enfatizar las acciones de Estonia por implementar algunas medidas del Manual a nivel Unión Europea y a partir de ello comprender las deficiencias para la aplicación de ciertos mecanismos preventivos. Y a partir de esta idea, comenzar a trazar esa política de seguridad y defensa que puede ser posible para la Unión Europea y que termina siendo influenciada por el Manual de Tallin.

Esta última fase es la parte principal de la investigación pues parto de la idea que el Manual tiene un papel fundamental para la Unión Europea pues pone en la mesa debates que la misma Unión no había pensado o querido plantear y a partir de ellos crea una política de seguridad y defensa viable para la protección de su ciberespacio. Y con ello crear un instrumento que pueda ser la antesala a una legislación a nivel internacional.

Debo aclarar que, esta investigación se centra en las acciones tomadas por la Unión Europea y los efectos en la misma. Aunque Rusia también fue un elemento importante para la creación del Manual de Tallin, la mención es superficial. No quita el hecho de que Rusia es un actor muy influyente para muchas de las medidas tomadas por la Unión Europea y que se mencionan en la tesis pero quise partir del sujeto que tendrá más atribuciones en estos asuntos.

Capítulo 1

Nociones sobre el Ciberespacio

> *Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente […] No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos. No hemos elegido ningún gobierno, ni pretendemos tenerlo […] Declaro el espacio social global que estamos construyendo independiente por naturaleza de las tiranías que estáis buscando imponernos. No tenéis ningún derecho moral a gobernarnos ni poseéis métodos para hacernos cumplir vuestra ley que debamos temer verdaderamente. No nos conocéis, ni conocéis nuestro mundo. El Ciberespacio no se halla dentro de vuestras fronteras. No penséis que podéis construirlo, como si fuera un proyecto público de construcción. No podéis. Es un acto natural que crece de nuestras acciones colectivas.*
>
> *John Perry Barlow, "Declaración de independencia del Ciberespacio", 1996.*

El Ciberespacio representó, en un primer momento, una revolución tecnológica que cambiaría la forma de comunicación en el mundo moderno. Se transmutan las relaciones entre los individuos, los gobiernos, las industrias y otros actores a partir de una inevitable interconexión del mundo. El Ciberespacio transforma la interacción entre estos actores al grado en el que las fronteras se eliminan, se constituyen nuevas identidades y se crea una nueva coyuntura sobre estas actividades nuevas en el mundo no físico.

Los gobiernos, las sociedades, las empresas, lo medios de comunicación, entre otros, conviven dentro de este nuevo espacio. Es a partir del nuevo paradigma tecnológico que "un segmento específico de su sociedad, en interacción con la economía global y la geopolítica mundial, [materializa] un modo nuevo de producir, comunicar, gestionar y vivir".[1] Y aunque esta evolución digital puede tener beneficios a futuro también convierte a todos sus actores en un blanco fácil de ataques dentro de este nuevo espacio. Esto crea una conciencia respecto a los peligros que representa la era digital.

[1] Castells, Manuel (2000), *The Information Age: Economy, Society and Culture*, *Volume I: The Rise of the Network Society*, Oxford, Blackwell, 2nd, p.13

1.1 Ciberespacio e Internet

1.1.1 Internet

Para poder comprender cómo todo el nuevo contexto mundial se ha transformado, se debe analizar a partir de los conceptos básicos que son la Internet y el Ciberespacio, que junto a la Globalización, han modificado la forma en la que el mundo se comunica. Tanto Internet como Ciberespacio, han sido utilizados como sinónimos cuando no lo son, pese a la dependencia mutua.

Para diferenciarlos se debe tener en cuenta que el Ciberespacio, "evoca, o engendra, maneras de interactuar que antes no eran posibles"[2] entendiéndose que "es toda forma de interacción digital no necesariamente a través de la red de redes llamada Internet sino también el intercambio vía bluetooth, el uso de tarjetas de crédito o de controles remotos, etc."[3]

Mientras que la Internet[4], por otro lado, "es un medio de comunicación. La gente hace cosas <<en>> Internet, cosas que son en su mayor parte triviales, por más que no dejen de tener importancia. En Internet, la gente paga facturas, reserva mesa en restaurantes, consulta noticias o se comunica con sus familiares mediante correo electrónico o mensajería instantánea".[5]

El Ciberespacio es el espacio creado para funcionar en medios como lo es la Internet y este mismo depende de la infraestructura como son los cables submarinos o la fibra óptica. En sí, el Ciberespacio es todo lo que se construye una vez estando dentro de un medio cibernético (entiéndase bluetooth, control remoto, conexión wi-fi, internet):

> El Ciberespacio se refiere a un entorno no físico creado por equipos de cómputo unidos para interoperar en una red. En el Ciberespacio, los operadores del equipo pueden interactuar de manera similar al mundo real, a excepción que la interacción en el Ciberespacio no requiere del movimiento físico más allá que el de escribir. […] La Internet constituye el mayor ámbito del Ciberespacio. Aquí se incluyen la World Wide Web (Web), los grupos de noticias USENET

[2] *Ídem*

[3] Misseri, Lucas (2015); *Ciberespacio y praxis: algunas reflexiones ético-politicas;* Argentina, Kazak Ediciones p. 19

[4] La cuestión de Internet con respecto si es "la" o "el" la comprendo como el uso de artículos según el uso que se le requiera. "La Internet", tal cual el desglose de la palabras, es "red de redes". Internet es la interconexión de las redes. La Internet hace mención a esta red. Cuando en otros momentos se refiere a "el Internet" es al medio, a ese medio de comunicación mencionado en el párrafo.

[5] Lessig, Laerence (2009); *El Código 2.0;* Traficantes de sueños, Madrid, España, p. 147

> y la Internet Relay Chat (IRC). A cualquiera de ellos es posible acceder con un acceso inalámbrico a Internet o con cualquier tipo de red que se tenga a la mano.[6]

Internet fue creado por la necesidad de que el ejército estadounidense continuara comunicado sin ser interferido por el bando enemigo, los rusos. En 1958, el Ministerio de Defensa crea *Advanced Researchs Projects* (ARPA) conformado por más de 200 científicos de gran estatus y se le otorga un enorme presupuesto para poder crear una alternativa de comunicación, en este caso, a través de ordenadores. Para 1962, "el ARPA creó un programa de investigación computacional bajo la dirección de John Licklider, un científico del MIT (Massachusetts Institute of Technology)".[7] Y 5 años después se crea ARPANET, "un plan para crear una red de ordenadores"[8] en el que trabajaban los mejores equipos del MIT, el Natinonal Physics Laboratory (Reino Unido) y la Rand Corporation.

> En 1972 ARPANET se presentó en la First International Conference on Computers and Communication en Washington DC. Los científicos de ARPANET demostraron que el sistema era operativo creando una red de 40 puntos conectados en diferentes localizaciones. Esto estimuló la búsqueda en este campo y se crearon otras redes.[9]

Entre los años 1974 y 1982 se crean grandes redes entre las que se destacan:

- Telenet (1974): Versión comercial de ARPANET.
- Usenet (1979): Sistema abierto centrado en el e-mail y que aun funciona.
- Bitnet (1981): Unía las universidades americanas usando sistemas IBM.
- Eunet (1982): Unía Reino Unido, Escandinavia y Holanda.

Era un caos poder controlarlo todo con un solo lenguaje en la programación por lo que se adopta el sistema de protocolos, el TCP/IP creando

[6] ¿Qué es el Ciberespacio? (2010), *Interflicto*. Recuperado de: https://goo.gl/H9Zua1
[7] Historia de Internet (2015). *UPC*. Recuperado de: https://goo.gl/zrps8X
[8] *Ídem*
[9] *Ídem*

la Internet dando un mejor control a la navegación en las redes conectando todas las redes que se podían conectar en aquel momento. Este sistema conforma la arquitectura formada por 5 diferentes niveles o capas, como vemos en la siguiente tabla:

Tabla 1. Niveles del protocolo	
Aplicación	Están contenidos los protocolos SMTP, para el correo electrónico; FTP, para las transferencia de archivos; TELNET, para la conexión remota, y HTTP, Hypertext Transfer Protocol.
Transporte	Se comprende a los protocolos TCP y UDP, que se ocupan del manejo y el transporte de los datos en las redes.
Internet	Se ubica en el nivel de la red para enviar los paquetes de información.
Físico	Es el análogo al nivel físico del OSI. Se refiere a las transformaciones que se le hacen a la secuencias de bits para trasladarse de un lugar a otro.
Red	Es el correspondiente a la interfaz de la red. Cuando ya está en la red.
Fuente: Estrada, Adrián (2005); Protocolos TCP/IP, *CISCO: Tecnología y diseño*. Recuperado de: https://goo.gl/c6GJPt Nota: El funcionamiento es más complejo de lo que se muestra en el esquema anterior, fue simplificado con fin de comprender el funcionamiento del protocolo TCP/IP	

En 1980, los ordenadores personales comienzan a tener un gran auge. El número de usuarios también comenzó a crecer al igual que las empresas que funcionan solo dentro de Internet. En 1985, Internet ya era una tecnología que pocos conocían. El autor William Gibson populariza el concepto de Ciberespacio tras su novela *El Neuromancer*. En 1990, tras sus trabajos en el Centro Europeo de Investigaciones Nucleares (CERN), Tim Berners Lee, junto Robert Caillau, nombrar al nuevo sistema de búsqueda, almacenamiento y recuperación de datos (proyecto en el que trabajaban) como World Wide Web (WWW)[10]. Este nuevo sistema busca facilitar el acceso a la documentación existente a través de Internet.

En 1991, se presenta al público y a finales de ese mismo año ya existían 50 sitios en la web a nivel mundial, el siguiente año ya existían 150 sitios en línea. En 1993, se crea MOSAIC, el primer buscador de la red que se maneja a

[10] Historia de Internet. (2015). *CAD*. Recuperado de: https://goo.gl/U3w47P

partir de este nuevo protocolo y popularizando el uso de la WWW, además de que se agrega la biblioteca gráfica (imágenes y sonido) haciendo más fácil la navegación por Internet.

Para 1996, los buscadores se hacen más populares y acercan al público general haciendo crecer las actividades en línea, además de que las industrias de computadoras comenzaron a crear aparatos electrónicos más accesibles al público y que a su vez facilitaban el acceso a Internet hasta llegar al uso cotidiano que se tiene en estos días.

Ya a finales de los 90, la Internet se convierte en una forma popular de uso. El comercio electrónico también es uno de los sectores beneficiados tras el auge de Internet pues se crearon "portales exclusivamente dedicados a esta actividad – tales como eBay y Amazon, los cuales se mantienen operativos y en pleno crecimiento hasta el día de hoy."[11] La interacción del mundo con este nuevo lugar artificial comenzaba a ser mayor produciendo una gran transformación en estos nuevos desarrollos en un espacio donde trasladaría el mundo real al virtual. Esto trajo consigo la construcción de una nueva realidad que ha revolucionado totalmente el funcionamiento del mundo tanto para los sujetos o entidades.

1.1.2 Ciberespacio

El concepto de Ciberespacio tiene una larga historia. Se tienen antecedentes del concepto mucho antes de la concepción que tenemos en la actualidad. Un ejemplo de ello es la teoría de Noosfera[12] concebida a inicios del siglo XX por Vladimir Vernadski, un filosofó ruso que hablaba de una evolución a

11 Victoria, Luis (2012). La historia del comercio electrónico. *Lynkoo*. Recuperado de: https://goo.gl/jcH5Nq

[12]La teoría habla de que la noosfera habla de las fases de desarrollo de la Tierra. La primera fase es la geosfera (materia inanimada), la segunda fase es la biosfera (vida biológica) y la tercera es la noosfera (seres inteligentes con el medio en que viven). En esta tercera parte, Vernadski habla sobre el pensamiento científico que se acelera, modifica y controla lo "natural". Respecto a Teilhar, hablaba de que la Noosfera conducía al acto del pensamiento en donde el mundo estaría interconectado por el pensamiento y generaría una conciencia universal. Más allá de una "realidad virtual" a partir de la tecnología sería a partir del pensamiento del hombre para llegar a la super-mente y llegar a la realización del espíritu de la tierra. Hay que considerar que Teilhar era un teólogo, su percepción era más sobre la conciencia humana que una concepción tecnológica pero si podría representar una buena analogía de lo que muchos pretendieron y pretenden que sea Internet. Podríamos decir que el Ciberespacio es la nueva conciencia del pensamiento humano si vemos como se interactúa en él.

la conciencia universal y sería retomada por Pierre Teilhard de Chardin aproximadamente en 1950 para construir el concepto de espacio virtual. Otros filósofos y científicos plantearían un concepto similar en ese mismo período pero no es hasta la década de los 1980 que se conoce al Ciberespacio similar a las percepciones que en la actualidad se admiten.

El concepto tal cual de Ciberespacio, usado con una connotación similar a la que conocemos actualmente, fue en utilizado en la novela de William Gibson, El Neuromancer de 1984. En esta novela se cuenta la historia de un estafador que tras robarles a sus antiguos jefes fue obligado a desconectarse del Ciberespacio, al cual podía recurrir conectándose a través del sistema nervioso. La concepción fue un primer paso para retomar el concepto al momento de nombrar esta realidad virtual. Aun así, la concepción de Gibson eramás a considerar al Ciberespacio como una segunda vida, una "alucinación" en la que podrían participar millones de personas y con una capacidad monumental de almacenamiento:

> Ciberespacio: Una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones, por niños a quienes se les enseña altos conceptos matemáticos… una representación gráfica de la información abstraída de los bancos de datos de todos los ordenadores del sistema humano.[13]

Algunos elementos semejantes a lo que entendemos como Ciberespacio son:

- El mundo creado por Gibson es un mundo dependiente del Ciberespacio pues todas las actividades del mundo real al mundo virtual están entrelazadas y no funciona una sin la otra. Actualmente, muchas de las actividades del Estado dependen del Ciberespacio[14]como servicios básicos; redes de información; instalaciones espaciales; industria química y nuclear; instalaciones de tratamiento de agua; centrales de redes y energía; tecnologías de la información y las comunicaciones; salud; transportes (puertos, aeropuertos, sistemas de control de tráfico); sistema financiero y tributario; etcétera.

[13] Bryant, Rebecca (2001), "What Kind of Space is Cyberspace?"; *An Internet Journal of Philosophy*, Vol. 5, p. 139

[14]La Infraestructura crítica se hablará en el apartado: 1.2.1 Infraestructuras Críticas.

- La creación de una sociedad que se mantiene conectada en este nuevo espacio social, además de la creación de una subcultura como es el cyberpunk. En nuestro espacio se han creado diferentes ciberculturas que conviven entre ellas pese a sus gustos y aun así pueden mantener su propia identidad.
- El poderío de multinacionales que ha llegado a modificar el comportamiento de la sociedad mundial en el futuro. Si recapitulamos la idea de las plataformas de negocio, como se puede ver en la **imagen 1**, podemos decir que estas mismas tienen un poder social tan grande que ha transformado la forma en que funcionan de muchos negocios. Por ejemplo, Facebook es una red social que tiene una influencia muy grande tanto a nivel virtual como físico, además de que ha modificado muchos comportamientos en la sociedad actual.
- La seguridad del Ciberespacio. En la creación de Gibson, el control que se tiene en el Ciberespacio es mayor, el delito es bastante castigado y se toman medidas severas. A diferencia, en nuestra realidad virtual, el control existente con el Ciberespacio avanza lentamente, no se puede poner a la par con el desarrollo del mismo, aun así se pueden comprobar casos en los que la seguridad es muy rígida pero sigue siendo vulnerable en donde la única alternativa es no tener Internet para no ser trasgredido.

Imagen 1. Funcionamiento del E-Commerce

La evolución del Internet ha sido tan avanzada que ha logrado la creación de negocios en plataformas digitales. Y aunque los negocios pueden parecer similares a los ya existentes en el mundo físico, existen muchas diferencias. La nueva forma de hacer negocios, el pago de impuestos, la contratación de personas, la propiedad de material físico entre otros temas son las nuevas formas de interactuar en el Ciberespacio y que son solo una parte de todas las posibilidades que nos trae este nuevo espacio.

Fuente: Losa, Guillermo, "¿Qué tienen en común Netflix, Uber y Airbnb?", *El Observador,* Recuperado de: https://goo.gl/XuTVYa

El Ciberespacio no tiene un significado aceptado a nivel internacional aunque si existe definiciones que puede acercarnos a la idea de lo que es Ciberespacio como el que lo considera "un entorno no físico creado por equipos de cómputo unidos para inter-operar en una red"[15] en donde existe una interacción entre sus usuarios a partir de información que se puede compartir, explorar o comprar.

El Ciberespacio también logra entenderse como "un medio virtual de interacción que, a diferencia de otros espacios, posibilita la experiencia independiente de la presencia física"[16]. Esto conlleva a que continuamente se planteen discusiones sobre los efectos que este *espacio no físico* produce en el *espacio físico* con el propósito de comprender características propias de él. A partir de estas discusiones se ha comprendido que el Ciberespacio ha creado nuevos desafíos que ya no solo competen a un solo país o países que comparten fronteras sino a todo el mundo conectado sin importar lo lejos que esté uno de otro.

El Ciberespacio reconstruye tanto un nuevo espacio como la misma sociedad donde los usuarios se convierten en los nuevos actores recreando las actividades que conciben en el mundo físico como la educación, la investigación, la lucha social, la denuncia, el comercio, la creatividad cultural, los medios de comunicación, la política y hasta el crimen o delitos, convirtiendo al mundo en un hibrido entre lo real y lo virtual. El Ciberespacio se convierte en "las tierras virtuales, con vidas virtuales y sociedades virtuales"[17], transformándose en un espacio nuevo.

Si entendemos el nuevo espacio a partir de la geografía, donde *Espacio* (Espacio Geográfico) es "la extensión que contiene la materia existente, de la parte que ocupa un objeto sensible o de la capacidad de un terreno o lugar. Se trata de cualquier sitio que sea habitado, modificado o transformado por el ser humano con el objetivo de obtener algún beneficio."[18]Aunque este término

[15]¿Qué es el Ciberespacio? (2010) Interflicto.com Recuperado de: https://goo.gl/wwvwx3

[16]Tellez Acuña, Fredy Reynaldo (2016); Prefijo Ciber: Arqueología de su presencia en la sociedad del conocimiento; *Universidad Nacional Abierta y a Distancia; (*No. 8) pp. 150-157

[17] Secretaría de Marina Armada (2015), *Seguridad y Defensa en el Ciberespacio*, Secretaría de Marina, México, Centro Superior de Estudios Navales (Ed.) p.22

[18] Pérez Porto, Julian (18 de mayo de 2017), Espacio Geográfico, *Ecured*, recuperado; de https://goo.gl/C6McZy

puede variar según las interpretaciones que le sean dadas. En el caso del geógrafo francés, Jean Tricart, se define *Espacio* (Espacio Geográfico) como:

> El resultado de la historia, ya que cada sociedad tiene su propio modo de organización y deja sus huellas en el paisaje. El espacio geográfico, por lo tanto, depende del proceso histórico. […] Cabe mencionar que para que exista un espacio geográfico debe haber, en primer lugar, un espacio natural que sirva de punto de asentamiento y desarrollo a una sociedad.[19]

El *Espacio* en si es el territorio, la historia, la política y la sociedad que existen dentro de él como identidades socioculturales.[20] Aun así, este término está más apegado a la concepción física, lo tangible. No obstante, si entendemos el funcionamiento del Ciberespacio, este puede ser comprendido a partir de esta misma idea. Para poder entenderlo, se parte de los mismos fundamentos y vislumbramos el nuevo concepto de Espacio Virtual donde se hará un estudio del Ciberespacio y las afectaciones políticas y socioculturales creadas.

En este caso, el estudio que comprende al Ciberespacio es la cibergeografía. Esta comprende como "espacio natural" el Internet y el ciberespacio. Esta rama de la geografía considera al Ciberespacio como un espacio, algo similar al espacio geográfico pero en lo virtual. Percibe al Ciberespacio como un nuevo espacio social donde las diferentes líneas de estudio se enfocan en cuestiones como infraestructuras físicas de la tecnología de la información y la comunicación, el espacio funcional entre los flujos de información a nivel global, los aspectos sociales y demográficos de las nuevas comunidades virtuales y como se comprenden los nuevos espacios virtuales. Se puede apreciar el trabajo de la ciberografía en los **mapas 1 y 2**.

El *Espacio Virtual*, se puede "comprender a partir del concepto según el cual lo virtual es un sistema o interfaz informático que se encarga de generar entornos sintéticos que se suceden en tiempo real"[21], es decir, lo que existe en lo real es representado en lo virtual:

---

[19] *Ídem*.

[20] Cfr. Cabeza Morillo, Hilda (2015); "Territorio y espacio geográfico", *Revista de Facultad de Ciencias Jurídicas y Políticas de la Universidad de los Andes,* Vol. 3, p. 6

[21] Rodríguez U., Migue Luis (2011, 7 de mayo), Poder Virtual como espacio geopolítico, *Geopolítica XXI*. Recuperado de: https://goo.gl/i3ypgG

> Es una representación gráfica y visible de determinadas cosas, situaciones, a través de medios electrónicos. […] El surgimiento de la problemática virtual, de los espacios y ambientes virtuales, ha venido a cuestionar la existencia de la realidad y a redefinir su naturaleza. Lo virtual es también real.[22]

En este también se recrean las relaciones sociales pero de una manera diferente en donde:

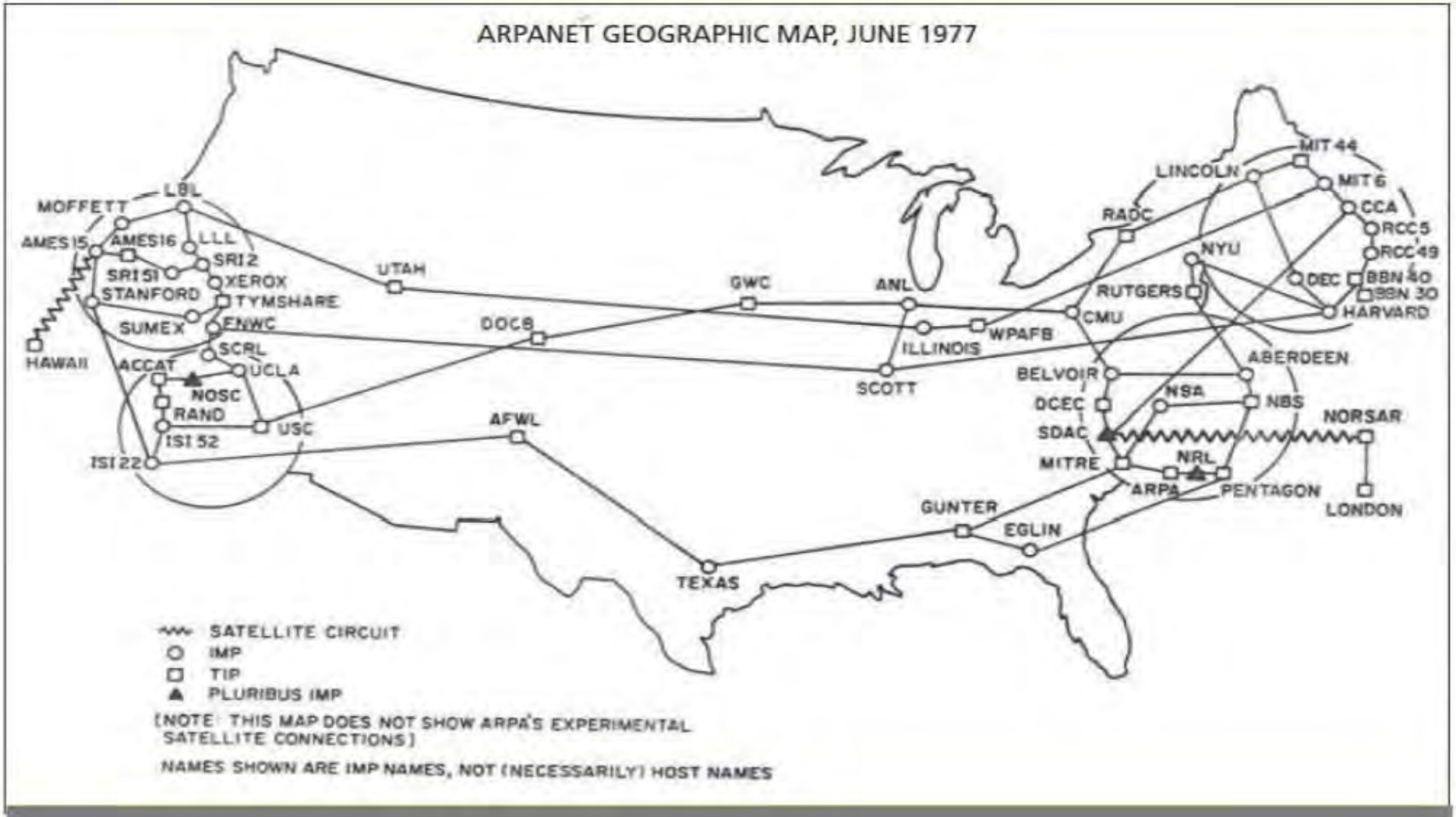
> […] la expresión de una relación asimétrica entre dos o más actores del sistema, sobre la base de lenguajes y de códigos de referencia virtuales que se traspasan a la realidad económica, social, política y territorial. […] se encuentra totalmente eliminada la frontera que sí existe en el "mundo real". Se alimenta y se ve influida por lo que acontece en el mundo físico, real. Los espacios virtuales dan cabida a formas de poder (económico, tecnológico, cultural e ideológico) que se despliegan al mismo hacia y desde los espacios territoriales materialmente existente.[23]

Para este punto se debe comprender que el espacio virtual tiene una gran relevancia el espacio físico afectando en gran medida su entorno. No puede suplantarse un espacio por otro debido a la dependencia entre ambos y así mismo cómo existen amenazas en el mundo real, el mundo virtual no se salva de las mismas, y muchas veces este mundo virtual es más vulnerable debido a esa falta de regulación en un espacio creado por todo el mundo.

Es así como se comprende que, Ciberespacio es el Espacio Virtual que se ha creado a partir de Internet, es el espacio donde el entorno virtual y las relaciones socioculturales -económicas, políticas, jurídicas, entre otras-, funcionan de manera parecida al espacio tangible y por ello, es necesario vislumbrar la importancia de toda la actividad que puede existir en este espacio y las consecuencias que puede tener para el espacio real. Por ello es tan necesaria su exploración pues, como en el espacio físico, se busca tener un dominio de este mismo que aventaje a un actor sobre otro al momento de un desacuerdo que podría convertirse en un conflicto en el Ciberespacio.

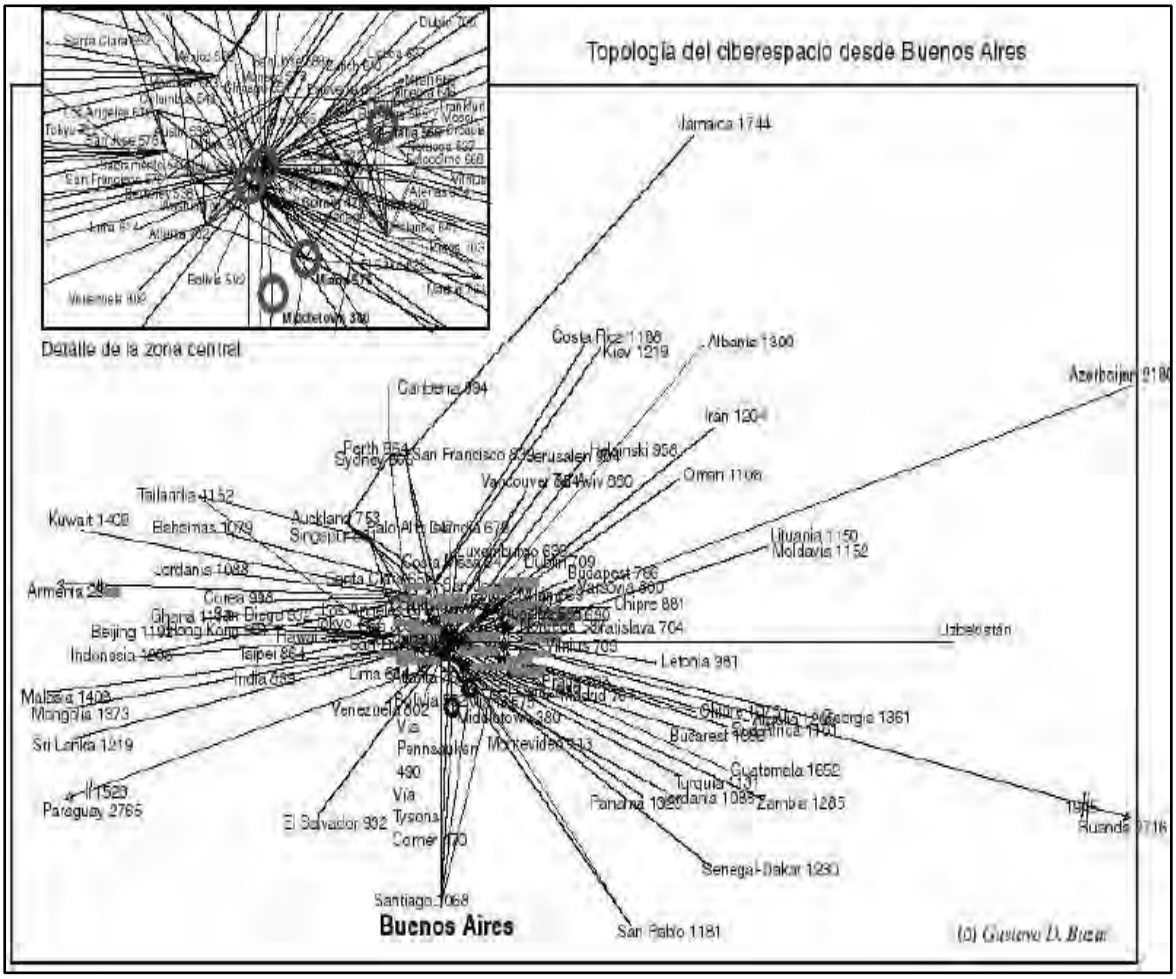
[22] *Ídem*
[23] *Ídem*

Mapa 1. Primer mapa del ciberespacio



Este el primer mapa que representa las primeras conexiones que existieron a partir de ARPANET.**Fuente:** Dodge Martin (2001); *Atlas of cyberspace*; Pearson Education Ltd, Inglaterra, p. 32

Mapa 2. Topografía del Ciberespacio desde Buenos Aires.



La cartografía del Ciberespacio se encarga de conocer todo lo que compone el Ciberespacio buscando crear un mapa a partir de las conexiones "lineales del espacio relacional, los vínculos entre lugares, sus posiciones relativas y las distancias ciberespaciales medidas en el tiempo". El tener un mapa del Ciberespacio completo una herramienta importante pues permitiría un mejor manejo de las herramientas con las que se cuenta para mantener un control de este mismo.

Fuente: Buzai, Gustavo (2012); "El Ciberespacio desde la Geografía. Nuevos espacios de vigilancia y control global", *Revista de Geografía Meridiano,* (No. 1), p. 237

1.2 Sobre amenazas tradicionales y asimétricas

Desde un inicio se ha considerado riesgo o amenaza a la seguridad nacional aquello que atente contra el Estado. Es así como los gobiernos han tomado medidas para el control de sus riesgos. La Seguridad Nacional es una de las funciones principales del Estado. Se debe enfocar en tomar medidas preventivas que garanticen la defensa de la soberanía, el cumplimiento del plan nacional y el eficiente desarrollo de la población. No obstante, en los últimos años, las amenazas han evolucionado convirtiéndose en preocupaciones a nivel regional, bilateral, multilateral o hemisféricas.

A lo largo de la historia las amenazas se han ido transformando según el desarrollo de la historia del ser humano. Las amenazas se han dividido en *amenazas tradicionales* (heredadas por la Guerra Fría) y *nuevas amenazas* (asimétricas). La cuestión, es que las amenazas a la seguridad han evolucionado a un punto en el que ya no son solo competencia de los Estados sino que obliga a todos los actores internacionales a cooperar para defender sus intereses. A veces estos mismos actores también se transforman en amenazas para la seguridad en cualquier nivel. Los espacios donde surgen estas amenazas también son cambiantes: las fronteras territoriales, el mar, el espacio exterior y en la actualidad el Ciberespacio.

Cada Estado tiene el derecho de identificar las prioridades nacionales de seguridad para poder definir estrategias o planes que puedan enfrentar estas amenazas. La diferencia entre las amenazas tradicionales y las nuevas amenazas es tanto la temporalidad, los actores y hasta el mismo espacio. Las amenazas tradicionales comúnmente era todo aquello que le podía afectar al Estado, podría ser otro Estado, movimientos internos contra el gobierno, la definición de territorio terrestre y marítimo. Al único que le competía crear planes de prevención sería al propio Estado.

Podría decirse que en el conflicto tradicional existen reglas para actuar debido a que hay varios tratados de guerra en donde se plantean, por decirlo de alguna forma, los pasos a seguir en una guerra como el respeto a los civiles o los derechos humanos. Aunque es claro que en una guerra esos principios muchas veces se violan, si están regulados y se castigarán como crímenes de guerra, a diferencia del asimétrico en donde no hay un concepto claro en

algunas de estas amenazas. Y al no ser conceptos claros, no se tiene un acuerdo internacional de permita su regulación aunque si hay intentos.

Lo que respecta a las nuevas amenazas, quienes pueden amenazar al Estado ya no son otros Estados o algún actor interno que buscara el desequilibrio del propio Estado, sino otros actores como grupos terroristas, narcotráfico o hackers. El conflicto convencional se transforma en un conflicto asimétrico. En el conflicto asimétrico ya no existe una igualdad al momento del enfrentamiento sino una diferencia enorme en cuanto a recursos de cualquier tipo: militar, político o mediáticos.

Por ejemplo, en la ciberguerra puede ser un solo individuo con habilidades en la programación y en todas las cuestiones informáticas para enfrentarse a un Estado. No hay un equilibrio en el equipo que puede tener un individuo en casa al de un país pese a ello la amenaza es evidente sobre todo si atenta contra cualquier sector del Estado.

O la cuestión del transporte marítimo en el Ártico[24] en donde la amenaza es a nivel hemisférico. Los planes de prevención tienen que ser a nivel hemisférico e incluso, si se agrava la situación, se convertiría en un problema global. La seguridad, en cualquier aspecto, ya no compete solo a un nivel, como lo es el nacional. Evoluciona a estos niveles[25] y crea diferentes tipos de cooperaciones para prevenir cualquier amenaza. En especial cuando se tienen objetivos similares a enfrentar y que siguen evolucionando con gran rapidez.

- Amenazas Tradicionales

Puntos de fricción entre Estados, conflictos con la delimitación de territorio terrestre como marítimo con países limítrofes, supervivencia por la falta de recursos naturales indispensables, etcétera.

[24] En los últimos años, con el derretimiento de los polos, se han creado rutas marítimas que están siendo aprovechadas por diferentes países para transportar mercancía de una manera más rápida. Estas nuevas rutas acortan el trayecto entre diferentes puntos comerciales importantes. Debido a esa facilidad, cada vez más hay más transporte marítimo comercial en esas rutas afectando el ecosistema y acelerando el derretimiento del Ártico. Por ello se están promoviendo planes para regular estas nuevas rutas pues podrían pasar de ser un problema hemisférico a un problema global.

[25] Los ya mencionados: bilateral, regional, multilateral, hemisférica, global, entre otros.

- Nuevas Amenazas

Proliferación masiva de armas de destrucción masiva, crimen organizado tradicional, narcotráfico, tráfico ilícito de armas y personas, terrorismo internacional, lavado de dinero, ataques al Ciberespacio, calentamiento global, entre otros.

1.3 Ciberespacio como nuevo campo de batalla: Infraestructura crítica, ciberataque, ciberseguridad, ciberguerra, Ciberdefensa y ciberestrategia

Aunque se mencionó que el Ciberespacio es un nuevo espacio social, no se podría concebir, en otros ámbitos, como un espacio similar al espacio geográfico. Esto es debido a que el Ciberespacio no contiene límites geográficos como el espacio físico y por ello no podemos considerarlo como un nuevo espacio sin gobierno pues se ha constituido a partir de los actores y factores que lo componen en todos los niveles. Podría decirse que se autorregula, aún así hay instituciones (públicas o privadas) que controlan gran parte de las funciones del mismo, de ahí que existan demasiados problemas al momento de querer intervenirlo.

El Ciberespacio se puede estudiar como nuevo espacio de interacción, como se mencionó inicialmente, pero el Ciberespacio no constituye un espacio en sí mismo "sino una dimensión que atraviesa los espacios físicos".[26] No es algo tangible pues todas las consecuencias de las acciones efectuadas dentro de este recaen en el mundo físico y no en su propio espacio, no cabe duda que las acciones dentro del Ciberespacio siempre son de preocupación. "[Es por ello que se puede considerar una amenaza] a la seguridad de los Estados donde subyace la superposición de los ámbitos de la seguridad interior y la defensa externa".[27] [28]

Pero el ciberespacio no puede concretarse a partir de la nada. Para que su existencia pueda ser plausible se tiene que tomar en cuenta la

[26] Eissa, Sergio Gabriel (2014), El Ciberespacio y sus implicancias para la defensa nacional. Aproximaciones al caso argentino, *Revista de Ciencias Sociales, segunda época*, (Nº 25), pp. 193-195

[27] *Ibíd*. p. 193

[28] Si la cibergeografía continúa con sus trabajos de mapear el Ciberespacio, es posible que el Ciberespacio tenga un valor geopolítico importante.

infraestructura física. Es a partir de su tratamiento que es posible la existencia del Ciberespacio. Existen 2 Infraestructuras físicas importantes, que además otorgan servicios de telecomunicaciones a diferentes niveles.

- Cable submarino[29]

Son los cables que permiten la conexión intercontinental a Internet. Estos cables son la principal Infraestructura que permite la conexión en el mundo. Estos cables se encuentran en los océanos a profundidad y son instalados por buques cableros que se encargan de conectar estos cables entre continentes. Uno de los más conocidos es MAREA, un clave submarino que conecta a España con Estados Unidos y es financiado por Facebook, Microsoft y Telefónica. Los cables submarinos son las autopistas que componen Internet.

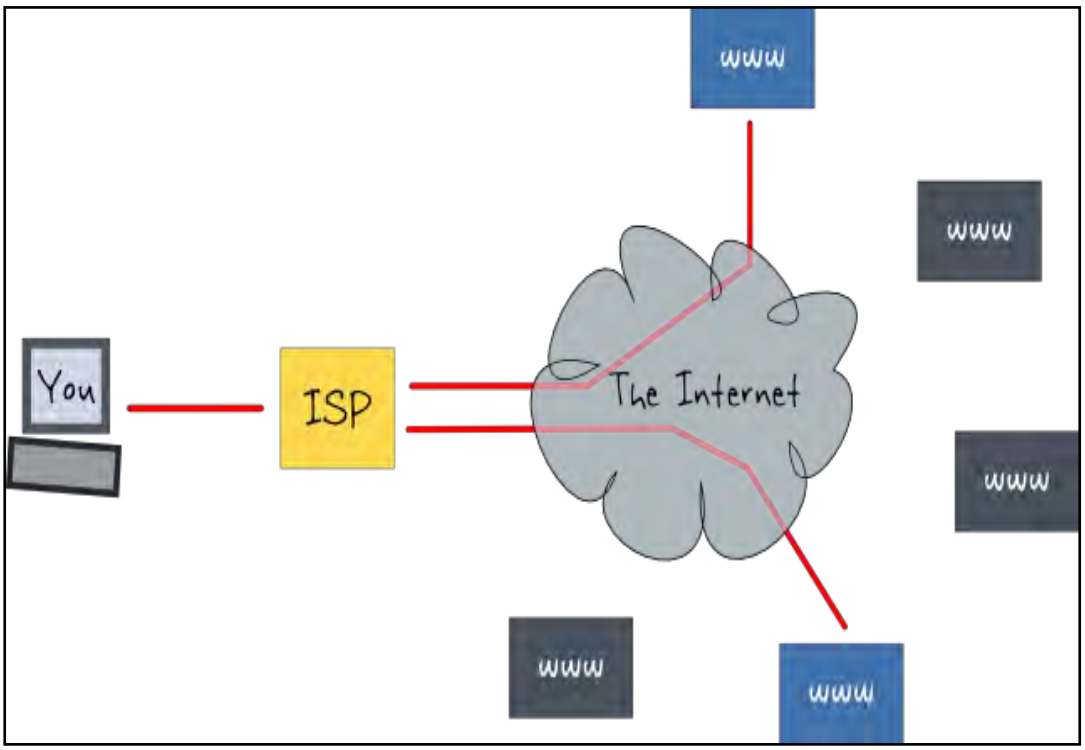
En los **mapas 3 y 4** podremos observar la representación de los cables submarinos actuales y los que se planean poner en un futuro. Esos mapas representan la importancia de los mismos cables submarinos en el mundo, en especial de forma geopolítica. Su ubicación y la pertenencia de los mismos influyen en el tráfico en internet.

- Proveedores de Servicio de Internet (PSI)

Estos más que Infraestructura física es más bien la administración del mismo internet. Estas empresas son las que permiten la conexión a internet a las personas. También son las encargadas, en su mayoría de colocar los cables submarinos para la distribución de servicios como lo es de telefonía, televisión por cable, Wi-fi, entre otros. Estos mismos PSI han causado gran controversia sobre su funcionamiento pues dependiendo del país y la empresa permite diferentes tipos de páginas a las cuales el usuario puede ingresar. Un PSI te permite entrar a diversas páginas o tiene un control de las páginas que se suelen visitar en un país, por lo que provoca cierta controversia el control de nuestra forma de navegar en el ciberespacio pues no es tan libre como uno podría imaginar. Podemos ver su funcionamiento en la siguiente imagen.

[29] En algún momento se llegó a acusar a Rusia de atacar cables submarinos de occidente y se le culpó de tratar de dañar Infraestructura de Red. Sobre el caso no hubo pruebas suficientes que permitieran una sentencia para Rusia debido a lo complejo que es destruir un cable submarino y que realmente son las empresas de los buques cableros las encargadas de arreglar los mismos.

Imagen 2. Funcionamiento de PSI (ISP por sus siglas en inglés)

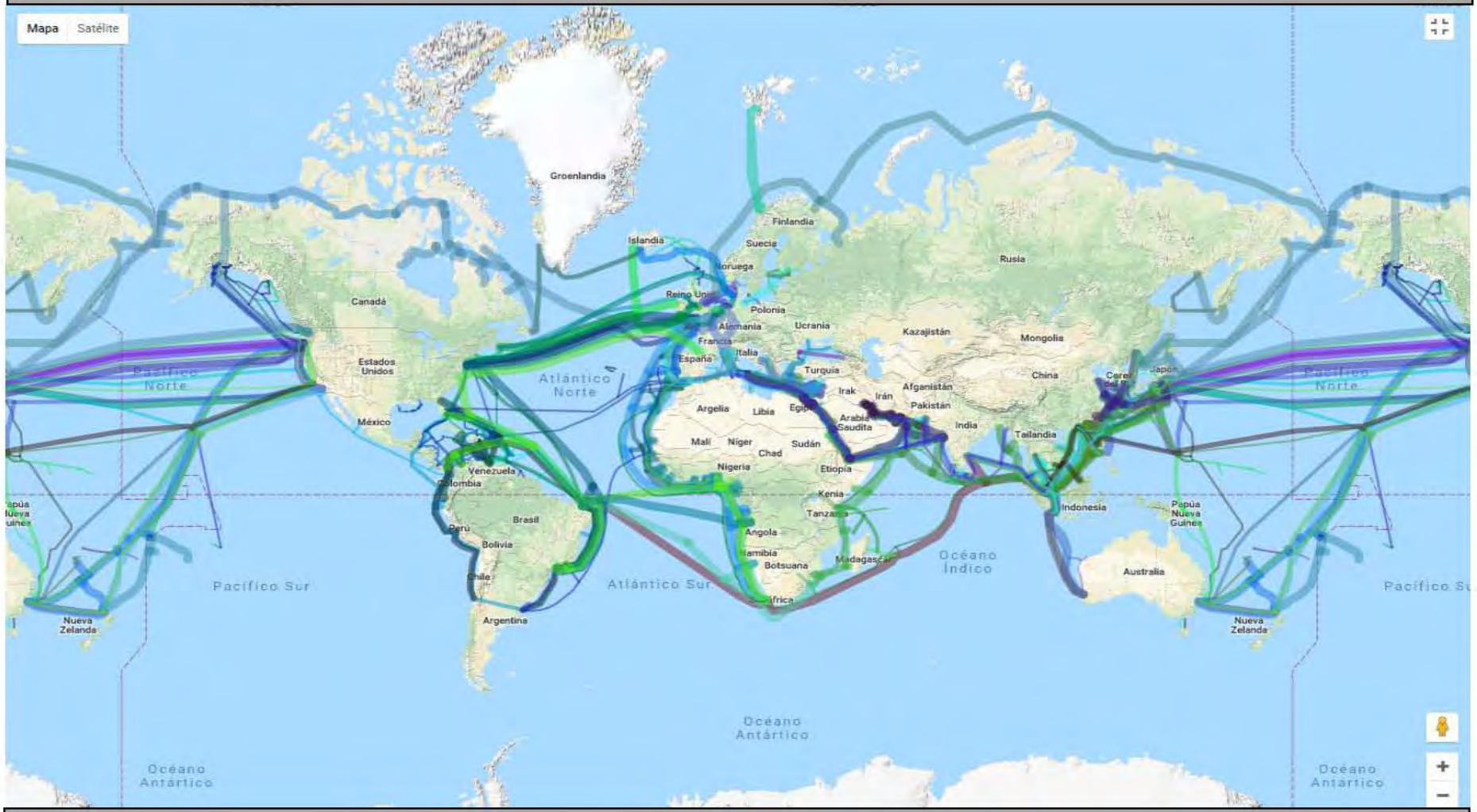


Fuente: Editorial (2012), Funcionamiento del ISP, *Manureva*h, Recuperado de: https://goo.gl/TQGGjW

Mapa 3. Mapa de cables submarinos activos

Fuente: Malknecht, Greg (2010), Mapa de cables submarinos, *Cablemap.*. Recuperado de: https://goo.gl/ZshhWz

Mapa 4. Mapa de cables submarinos futuros



Fuente: Malknecht, Greg (2010), Mapa de cables submarinos, *Cablemap. R*ecuperado de**:** https://goo.gl/ZshhWz

Estas infraestructuras permiten la conectividad al mundo y un ataque a las mismas podrían provocar el colapso del ciberespacio[30]. Las infraestructuras físicas como las cibernéticas permiten que el funcionamiento del ciberespacio sea posible y permita que se constituya un nuevo espacio de interacción como el que orgánicamente se crea en el ciberespacio. Y hay que comprender que pese a que el ciberespacio no tiene fronteras dentro de sí, sí existen formas de dividirse en el mundo: ya sea por pertenencias, espacio geográfico o fronteras físicas. Es así como también se debe comprender que existen dos tipos de Infraestructura Crítica (IC): las que pertenecen al Estado y las que son de Internet, que pueden pertenecer al Estado pero en su mayoría son acuerdos comerciales y pertenecen a empresas privadas o en colaboración entre lo privado y público reguladas por el Derecho Internacional.

Por ello, los ataques a cualquier infraestructura son necesarios de comprender. Pues tienen diferentes variables, en este caso el físico y cibernético. A diferencia de lo que se cree, los ataques físicos ya han sido estudiados desde hace muchos años pues se comprenden dentro de las Estrategias Nacionales de Seguridad y son los sectores más importantes para un Estado. Por ello, las industrias de seguridad ya ofrecen servicios para la protección de la IC. Los ataques físicos son más sencillos de detectar y son limitados pues no es posible el ataque simultáneo a todas las IC de un país.

El segundo tipo es el ataque cibernético, en donde se atacan las IC desde el Ciberespacio. A diferencia del físico, el cibernético si podría tener un efecto más letal pues sus formas de ataque son ilimitadas. Si se desea atacar a diferentes sectores de la IC es posible que existan efectos cruzados y producir un grave daño. “La información manejada por las redes informáticas (que son las que gestionan nuestros servicios públicos, nuestro transporte, nuestra banca y nuestras comunicaciones) pueden ser aprovechadas o atacadas en segundos desde una ubicación remota en el extranjero”.[31]

La evolución de las amenazas tradicionales a asimétricas es más clara en el Ciberespacio. Estas amenazas han modificado la necesidad de

[30] En las primaveras árabes, por ejemplo, fueron cortadas varias infraestructuras físicas que ayudan a conectar a la red para evitar el envío de información a la red. Pero varios colaboradores europeos lograron crear una red a partir de aparatos viejos que permitieron continuar con la comunicación en red de varios países.

[31] Clarke, Richard A. (2015), *Guerra en la red: los nuevos campos de batalla*, Ariel, España, p. 71

protección debido a lo sofisticado de los ataques, el anonimato de los actores y las capacidades de los mismos en el conflicto:

> Las operaciones cibernéticas constituyen amenazas a la ciberseguridad en un sentido general o ampliado, lo que afecta un *estado de cosas deseable* en referencia a los sistemas informáticos de un Estado. Sin embargo, solo una porción de estas operaciones afecta específicamente el ámbito de la defensa nacional. […] dentro de la amplia gama de operaciones cibernéticas, únicamente son de interés para la defensa nacional aquellas que persiguen objetivos militares, es decir, que poseen la intención de alterar e impedir el funcionamiento de las capacidades del sistema de defensa nacional. Por lo tanto, aquellas agresiones que afecten toda otra infraestructura que no pertenezca al sistema de defensa nacional son responsabilidad, en primera instancia, de otras agencias del Estado.[32]

La ciberseguridad se ha tornado tan importante que en algunos países ya existe algún apartado en la estrategia nacional de seguridad que se refiera al Ciberespacio debido al gran impacto que este espacio tiene, ya no solo a nivel nacional sino a nivel internacional. "[Con] fin de evitar impactos no previstos derivados de la falta de madurez regulatoria y procedimental y del creciente número de amenazas ciber, los estados soberanos comienzan a disponer de estrategias integrales de ciberseguridad a través de una hibridación jurídico-técnica, tanto en el entorno empresarial como sectorial. Con más de 27 ciberestrategias a escala mundial […]"[33]

> Entre los diferentes países que tienen una estrategia desarrollada de ciberseguridad se encuentran "los Five Eyes (Canadá, Estados Unidos, Reino Unido, Nueva Zelanda y Australia), los países europeos estratégicos miembros de la Alianza Atlántica en términos ciber (como Estonia) o la emergente América Latina, con Brasil a la cabeza. [En] los países asiáticos, [teniendo] aproximaciones intervencionistas sobre su Ciberespacio, [se encuentran] China o Irán […] En este escenario nacieron las primeras estrategias nacionales de ciberseguridad […] entre el bienio 2011-2013.[34]

Se debe concebir al Ciberespacio y su seguridad como temas muy complicados a nivel internacional en las cuestiones políticas y jurídicas, principalmente. Debido a los constantes ataques recibidos en el mundo dentro

[32] Eissa, Sergio Gabriel, Op. Cit., pp. 193-195
[33] Hernández, Adolfo; Estrategias nacionales de ciberseguridad en el mundo; *Red de Seguridad*; Recuperado de: https://goo.gl/r8EGu1
[34] *Ídem*

del Ciberespacio se tienen que tener precauciones al respecto, pues el Ciberespacio no solo es atacado de forma virtual sino que también puede tener sus daños en el mundo real. Es importante recordar que lo señalado anteriormente, el espacio virtual y el físico, siempre están correlacionados pues si llegase a afectar la infraestructura física del Ciberespacio[35], el mismo tendría problemas de funcionamiento, además de tener efectos negativos en la infraestructura crítica de la cual los Estados dependen.

1.3.1 Infraestructura Crítica

Una de las partes primordiales para los estados son las Infraestructuras Críticas (IC)[36], estas son "todas aquellas estructuras, servicios y sus componentes informáticos que permiten a una sociedad moderna mantenerse conectada y funcionando: […] desde la red eléctrica, carreteras, puentes, aeropuertos, puertos, fuentes de agua y alimentos, servicios de salud, sistema financiero y de transporte, además de la red cibernética. [sic]"[37] Esto obliga, al Estado, a proteger estas Infraestructuras de cualquier tipo de ataque, en especial ahora que son más dependientes de las conexiones con el Ciberespacio.

Los ataques cibernéticos a Estonia en 2007 o Georgia en 2008, representaron una invasión a sus IC, y aunque en estos casos no hubo una invasión a las infraestructuras más importantes, si representó una primera advertencia de lo frágil que puede ser un Estado sin la protección necesaria a estos elementos. Los ataques posteriores, a Irán, si pudieron tener graves consecuencias, lo que demuestra las debilidades del Estado en el Ciberespacio que aún sigue regulándose respecto a este tema a paso lento mientras que el mismo Ciberespacio evoluciona con más velocidad, al igual que los ataques posibles creando la necesidad de establecer mecanismos que protejan al Ciberespacio, tanto a nivel nacional como a nivel internacional.

---

[35] Como cables submarinos y Proveedores de Servicio de Internet

[36] Cada Estado cuenta con diferentes Infraestructuras Críticas por lo que no siempre serán los mismos sectores de interés. Aun así se pueden deducir pues hay sectores de máxima prioridad para casi todos los Estados que coinciden.

[37] Hernández, Adolfo; Estrategias nacionales de ciberseguridad en el mundo; *Red de Seguridad*; Recuperado de: https://goo.gl/ZovfgK

Los ataques cibernéticos han representado un gran reto para los Estados debido al poco control que pueden ejercer al momento de detener un ataque a sus infraestructuras críticas. En 2010, el programa nuclear de Irán fue atacado por el virus de Stuxnet lanzado por Estados Unidos e Israel. Este ataque causó uno de los más grandes daños a su infraestructura nuclear provocando que Irán buscara especializarse en la protección de estas centrales nucleares, y en general de toda su infraestructura que podía ser vulnerada en algún momento. En 2016, logró controlar ataques cibernéticos que se dirigían a sus plantas petroquímicas, que meses atrás a ese incidente habían provocado incendios de graves consecuencias. Y aunque no son los únicos casos de ataque que ha recIbido el país, la necesidad de protección es latente y buscan actualizarse constantemente para mantener sus infraestructuras críticas seguras sin daños mayores.

La fragilidad que representa la infraestructura crítica, conectada al ciberespacio, para un Estado puede representar miles de pérdidas, tanto económicas como políticas como de seguridad. Con el ejemplo de Irán, los ataques son dirigidos especialmente a su industria petrolera debido a que la República Islámica busca recuperar su economía a partir del petróleo y el gas pero son obstaculizados por occidente constantemente a través de ataques cibernéticos que facilitan una guerra silenciosa y en un espacio poco protegido donde los actores pueden permanecer en el anonimato o son difícilmente identificados.

Los ciberataques que tienen el propósito de afectar las infraestructuras críticas directamente son muchos. Por ejemplo, el caso China en la Operación Aurora. Este fue un caso de ciberespionaje por parte de Estados Unidos a China. Cuando fue rastreado el espionaje y se acusó a Estado Unidos de ser quién lo dirigía. EU aseguró que realmente el ataque procedía de China pero fueron rastreados los servidores de Google, que estaban en China, comprobando que el robo de información era por parte de Estados Unidos.

Instalaron un *backdoor*[38] “en sus servidores para robar el código fuente de sus proyectos. Tras analizar en detalle el binario utilizado, se descubrió que utilizaban algoritmos de código de redundancia cíclica CRC de los que sólo

[38]Un tipo de Malware que se explicará más adelante.

había documentación en chino y además pudieron descubrir varias rutas que hacían referencia a un programa llamado Aurora".[39] Este incidente no llegó a mayores pero si dejó en claro que cualquiera puede ser una amenaza a la seguridad nacional, incluso una empresa como Google.

Como vemos, las Infraestructuras Críticas son necesarias para la actividad normal de los servicios básicos y la producción de cualquier sociedad. "De tal manera que cualquier interrupción no deseada, ya sea debida a causas naturales, técnicas, ya sea por ataques deliberados, tendrían graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, aparte de ser una fuente de perturbaciones graves en materia de seguridad".[40]

Para poder entender los problemas que ocasionaría un ataque cruzado en la IC, debemos tener 3 elementos para la protección de la IC. El primero es un mapa de riesgos en donde se tienen que tener en cuenta solo las amenazas posibles a la IC, lo que realmente podría ocurrir. Como segundo, la Arquitectura de la IC y sus conexiones al Ciberespacio (la geografía del Ciberespacio) en donde se consideren 3 redes importantes: la red corporativa[41], la red de servicios y la red de control. Estas 3 redes tienen que mantenerse separadas para que existan menos probabilidades de ataque masivo.[42]

Y tercero, las personas que tendrán el control de todo esto, quienes manejaran todas estas redes y estarán al tanto de los sistemas de control. Existe una diferencia entre el personal dedicado a la industria y el personal del Estado. El personal de la industria tiene como fin la ganancia, el Estado tiene como fin proteger al propio Estado. A veces ambos actores participarán en conjunto para la protección de las IC, por ello las personas que estarán encargadas de esto no tienen que ser un riesgo para la seguridad.

---

[39]Realpe Díaz, Milena Elizabeth (2016), *La ciberguerra, una amenaza a la Seguridad y Defensa Nacional*, Centro Superior de Estudios Navales (Ed.), Seguridad y Defensa en el Ciberespacio, Secretaría de Marina, México, p. 302-303

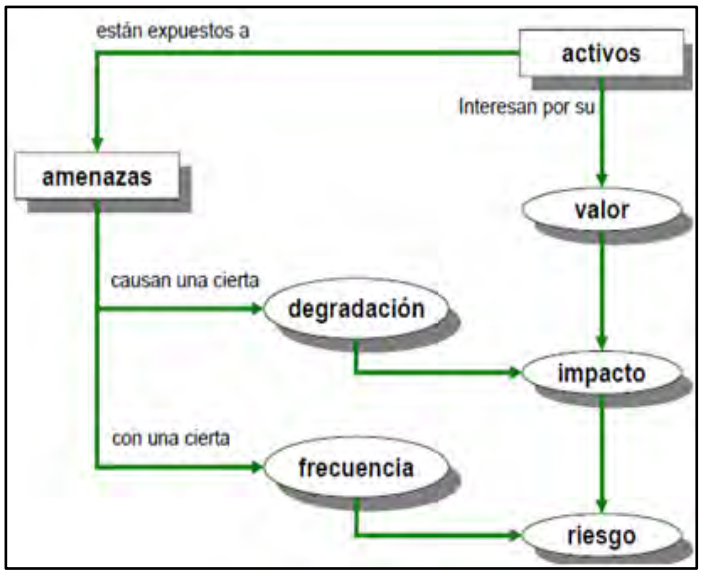
[40]Hernán Gómez de Mateo, José Luis (2014); Dilemas Cibernéticos y la Estrategia de Seguridad Nacional; *Instituto Español de Estudios Estratégicos*; España; p. 5

[41] Esta hace referencia a las empresas que están instaladas en un país. En el caso de ciberespionaje en China podemos percibir lo importante que es una red como de este tipo que puede vulnerar la seguridad de un país.

[42] *Cfr*. Universidad Rey Juan Carlos [unversidadujc] (2016). Concepto de infraestructura crítica y principales amenazas existentes [Archivo de video]. Recuperado de: https://goo.gl/mCMR1i

Una última cuestión con las Infraestructuras Críticas es la pertenencia de estas. En un primer momento su protección compete al Estado pero hay IC que no pertenecen al Estado sino al sector privado[43]. Por tanto, la seguridad de estas compete solo a las propias empresas. Aunque se puede seguir el mapa de riesgos para la protección de las IC, como ya se mencionó, la cooperación entre lo público y lo privado es inminente. Asimismo, el sector muchas veces tiene inversiones en el sector público en las infraestructuras.

Imagen 3: Esquema para la creación de un Mapa de Riesgos



Fuente: Hernández, Adolfo; *Estrategias nacionales de ciberseguridad en el mundo*; Red de Seguridad; Recuperado de: https://goo.gl/ZovfgK

Es un asunto importante a tomar en cuenta porque al competer empresas privadas en asuntos públicos, los riesgos son aún mayores y se necesita una verdadera y eficaz estrategia de seguridad para que no existan problemas a futuro. Agregando el tema de la conexión de IC al Ciberespacio, las posibilidades de riesgo son mayores. Tiene que existir una relación estrecha con lo privado para que el riesgo de pérdida sea menor pues aunque es una infraestructura privada podría afectar rotundamente a todos los componentes del Estado[44].

[43] En Argentina, el servicio de transporte está a cargo de las empresas privadas como: Santa Ana, Unión Bus, El Urbano Coop.

[44] Esto también dependerá de qué tipo de IC pertenezcan al sector privado y el grado de importancia para el Estado. El servicio de transporte, por ejemplo, puede representar un riesgo si existe un atentado terrorista y más si no se permite la injerencia del Estado para prevenir otra situación igual. La mayoría de las veces son las empresas privadas quienes están mejor preparadas para cualquier tipo de ataque (de menor medida a mayor) por ello el gobierno debe de mantener una relación estrecha con este sector para también enfrentar los problemas que podría existir en IC que solo controla el Estado. Aunque en la actualidad considero que existe una mayor injerencia en las empresas privadas y sus inversiones para la Infraestructura Pública, además de empresas de seguridad y ciberseguridad son contratadas por el mismo gobierno para la protección de estas. Y la seguridad privada también es un punto importante para analizar pues en la actualidad se tiene más confianza contratar a una empresa

1.3.2 Ciberataques

Un ciberataque se ha considera como un acto en el que se daña, perjudica o agravia en contra de las personas, entidades o instituciones, ejecutadas por medio de computadoras y a través de Internet. “Un ciberataque puede estar dirigido a los equipos y sistemas de computación que se encuentran operando en la red a nivel mundial, o puede ser orientado hacia la información y los datos que son almacenados en bases de datos”.[45] Los ataques pueden ir tanto contra los datos como con propósitos militares o comerciales. Debido a los diferentes propósitos que tiene un ciberataque, también existen diferentes tipos, unos pueden ser más severos que otros, dependiendo de la categoría de los mismos como se ven en los siguientes tablas:

Tabla 2. Tipos de ciberataque

Tipo	**Descripción**	
Malware	*Malware*	Software malicioso cuyo objetivo es infiltrarse a un sistema y dañarlo. Algunos ejemplos son los gusanos, troyanos, etc.
	Virus	El virus infecta los ficheros del sistema mediante un código maligno. Este necesita ser ejecutado por el usuario.
	Spyware	Es un programa espía, cuyo objetivo principal es obtener información. Trabaja de forma silenciosa de forma que no se vea que existe en el sistema e instalar programas sin consentimiento del usuario.
	Adware	Es la muestra de publicidad con intención de dañar equipos. Puede recopilar y transmitir datos.
	Ransomware	Software que se muestran datos y pedir un rescate por ellos en bitcoins, moneda local u otro tipo de moneda.
Pishing	Suplanta la identidad, generalmente en correo electrónico, mensajería o llamadas telefónicas.	
DDoS	Denegación de Servicio. Puede provocar tráfico inútil en la red provocando su colapso. Este ataque se da en los sitios web o servicios alojados en los servidores.	

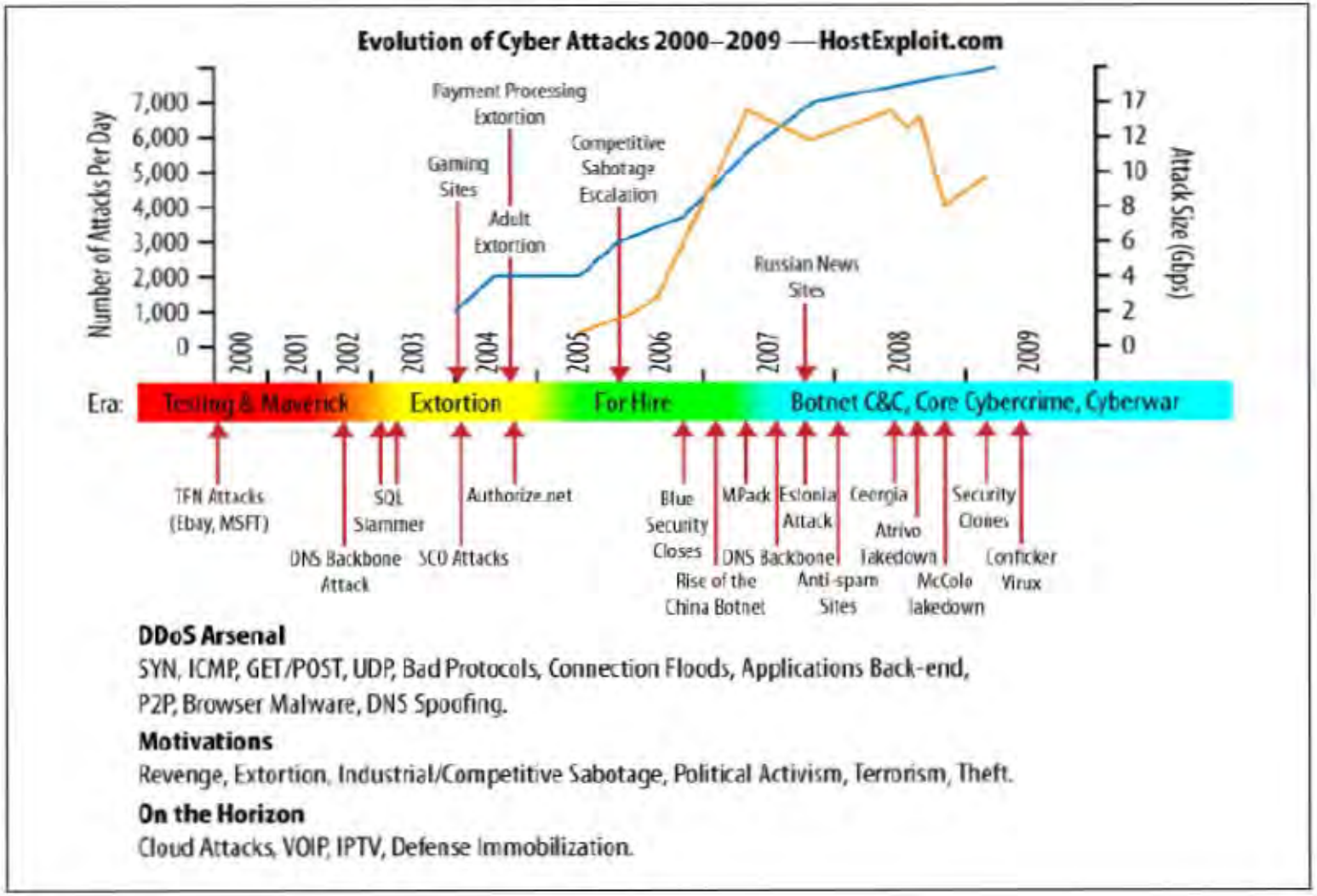
Fuente: Conde, Rubén (2018). Los Ciberataques: tipos y previsiones para 2018. *RCG Comunicaciones*, Recuperado de: https://goo.gl/nzFCMc

privada que confiar en la seguridad pública, es un punto a tomar en cuenta respecto a la seguridad de las IC pues hay un punto débil que combatir.

[45]Freet, Nahun (2015). ¿Qué es un ciberataque? Auditool. España, Recuperado de: https://goo.gl/CxZ3hs

Tabla 3. Categorías de Ciberataques		
Categoría	**Subcategoría**	**Ejemplos**
Integridad Los ciberataques pueden utilizar técnicas para modificar, destruir o hacer otras acciones que comprometan la integridad de los datos	Propaganda/ Información	Manipulación de datos contradictorios para influir en resultados políticos, de negocios o la desestabilización de un régimen extranjero
	Intimidación	Ataques a sitios web para coaccionar a los dueños (públicos o privados) para remover o modificar contenido.
	Destrucción	Destrucción permanente de datos para afectar competidores o atacar gobiernos extranjeros.
Disponibilidad Ataques de denegación de servicio ejecutados por botnets, por ejemplo, pueden ser utilizados para prevenir que usuarios accedan a datos que de otra manera no estarían disponibles	Información externa	Denegación de servicio. Ataques contra servicios de gobierno o privados disponibles para el público, como medios de comunicación, sitios de información o gubernamentales.
	Información Interna	Ataques a intranets gubernamentales o privadas como redes de servicio de emergencia, sitios de banca electrónica, correo corporativo, sistemas de control y comando.
Confidencialidad Los ciberataques pueden apuntar a varios tipos de información confidencial, regularmente para propósitos criminales	Espionaje	Firmas buscando información sobre sus competidores. Espionaje estatal.
	Robo de datos personales	Ataques de falsificadores dirigido a usuarios débiles para que revelen datos personales como números de cuentas bancarias, malware.
	Robo de identidad	Virus para robar información de identidad y usarla para cometer crímenes.
	Minería de datos	Técnicas de código abierto empleadas para descubrir información personal.
	Fraude	Generalmente se envía por correo electrónico mediante spam donde se busca convencer al destinatario de comprar servicios o bienes fraudulentos.

Fuente: DCAF (2009), Democratic Gobernance Challenge of Cyber Security, *DCAF*, Recuperado de: https://goo.gl/C6SDzD


Evolution of Cyber Attacks 2000–2009 —HostExploit.com
Number of Attacks Per Day
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
Attack Size (Gbps)
17
12
10
8
6
4
2
0
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
Payment Processing Extortion
Gaming Sites
Adult Extortion
Competitive Sabotage Escalation
Russian News Sites
Era:
Testing & Maverick
Extortion
For Hire
Botnet C&C, Core Cybercrime, Cyberwar
TFN Attacks (Ebay, MSFT)
DNS Backbone Attack
SQL Slammer
SCO Attacks
Authorize.net
Blue Security Closes
Rise of the China Botnet
MPack
DNS Backbone
Estonia Attack
Anti-spam Sites
Georgia
Atrivo Takedown
McColo Takedown
Security Clones
Conficker Virux
DDoS Arsenal
SYN, ICMP, GET/POST, UDP, Bad Protocols, Connection Floods, Applications Back-end, P2P, Browser Malware, DNS Spoofing.
Motivations
Revenge, Extortion, Industrial/Competitive Sabotage, Political Activism, Terrorism, Theft.
On the Horizon
Cloud Attacks, VOIP, IPTV, Defense Immobilization.

Los ciberataques han aumentado de manera exponencial, como se observa en la **imagen 4**, especialmente aquellos encargados de robar información confidencial tanto de los sectores industriales como de los Estados. Los ciberataques podrían considerarse la mayor amenaza en la actualidad debido a la interconectividad del mundo, lo que a su vez ha transformado las vulnerabilidades de un Estado. La dependencia a la tecnología "es prácticamente completa, cualquier falla o intrusión en un sistema informático puede causar daños irreparables"[46]. Aunque también hay que tener en claro, los ciberataques tienen sus limitaciones cuando se habla de aspectos masivos y su programación, aun así los daños que puede ocasionar son numerosos.

1.3.3 Ciberguerra

Julian Assange, en su libro Cypherpunks, hace una descripción corta de cómo el Ciberespacio comienza a ser usado como un campo de guerra. Al igual que en una guerra física, los soldados son entrenados para acatar órdenes a partir de las necesidades de un Estado.

Jacob Appelbaum[47], uno de los participantes en las entrevistas, habla sobre su experiencia en uno de estos campos de entrenamiento de soldados cibernéticos en el que prácticamente su entrenamiento es tanto dentro como fuera del Ciberespacio. Tienen que ser entrenados para derribar cualquier tipo de programa o sistema que funcione pueda llegar a atacarlos pero también tienen que mantenerse leales a un Estado que es a quienes sirven:

> Fue una sensación muy extraña porque te encontrabas frente a gente con bagaje bélico, que poseía conocimientos acerca de la guerra pero no enseñaba estrategia; solo se centraban en la retórica de defender estos sistemas, o en la de su ataque. Y tenían tanta guerra en el camino que por todos los medios trataban de enardecer el fervor patriótico de sus participantes. No fomentaban el pensamiento creativo ni algún tipo de marco para el análisis independiente; insertaban nuevas piezas en los engranajes mentales de quienes solo siguen órdenes dizque por el bien de la nación.[48]

[46]Uruena, Francisco (2015). Amenaza de los ciberataques. *Instituto Español de Estudios Estratégicos*. (No. 40), p. 15

[47]Fundador de Noisebridge en San Francisco, miembro del Club berlinés del Caos Informático y desarrollador.

[48] Assange, Julian. *Cypherpunks. Temas de hoy*. México-Estados Unidos. Editorial Planeta. p. 58-59

Estos son los nuevos ciberguerreros, aquellos que se enfrentaran en un campo de batalla virtual contra otro Estado. Este nuevo tipo de guerra no tiene necesidad de una declaración debido a las múltiples ventajas que el Ciberespacio le permite para moverse, empezando por el anonimato del ataque y el hecho de que no existe un límite fijo que impida atacar a otro en cuestión de segundos. Además, no se necesita personal para atacar de manera física, solo una computadora y un ciberguerrero.

> En términos muy generales, el hecho de que los ciberguerreros pueden introducirse en estas redes y controlarlas o hacerlas caer. Si se apoderan de una red, los ciberguerreros pueden robar toda la información que contiene o darle instrucciones para transferir dinero, derramar petróleo, liberar gas, volar generadores, descarrilar trenes, estrellar aviones, enviar pelotones a una emboscada o detonar un misil en el lugar equivocado. Si consiguen hacer caer una red, borrar datos e inutilizar ordenadores, los ciberguerreros pueden colapsar un sistema financiero, detener una cadena de abastecimiento, sacar un satélite de su órbita, inmovilizar una aerolínea.[49]

Desde la creación de Internet, el objetivo de uso de este medio sería para guerra. Este fue un medio creado para obtener ventaja al enemigo y poder demostrar superioridad tecnológica justo en la era de la Guerra Fría. Pese a ello, aún no se tenía claro la capacidad que tenía este nuevo medio para la guerra y en cuestión de unas décadas se pudo averiguar el impacto que este tiene y las consecuencias graves de las acciones realizadas dentro del Ciberespacio.

No obstante, algunos expertos del campo consideran que la ciberguerra puede ser una ficción pero la realidad es que ya es algo más latente cada día. Aunque no han existido casos de países pronunciándose de manera oficial contra otro, como en una guerra física, la realidad es que la interconexión del mundo te da las posibilidades de atacar sin ser identificado. Las veces que se ha considerado una ciberguerra no son pocas, pero si se ha identificado a los posibles responsables donde otros Estados son los autores del ciberataque por lo que no se puede negar que existe la ciberguerra aunque con normas totalmente diferentes a las acostumbradas.

[49]Clarke, Richard A., *Guerra en la red: los nuevos campos de batalla*, España, Ariel, p. 104

> La ciberguerra es global. En cualquier conflicto, los ciberataques pasan con rapidez a ser globales a medida que, por todo el mundo, ordenadores y servidores hackeados, o reclutados de forma encubierta, entraran en acción a la fuerza. Muchas naciones (…) se ven arrastradas a la confrontación […] La ciberguerra ha empezado (…) las naciones están ya <<preparándose en el campo de batalla>>. Están hackeando sus redes e infraestructuras unas a otras, dejando puertas traseras y bombas lógicas; ahora, en tiempos de paz. La vigencia de la ciberguerra, el hecho de que sea algo en desarrollo, que difumina los límites, entre la paz y la guerra, añade una dimensión de inestabilidad nueva y peligrosa.[50]

Tras todo lo mencionado, y debido a los debates de si existe o no una ciberguerra como tal, se debe señalar que no existe una definición clara de lo que es la ciberguerra, además de que esta tampoco cuenta con ciertas reglas como en su momento podría tener la guerra física. Algunos autores definen ciberguerra como el acto que tiene por objetivo el "encontrar vulnerabilidades técnicas en los sistemas o redes informáticas del enemigo para penetrarlas y atacarlas, tanto así como extraer datos e información sensible".[51]

Es así como el Ciberespacio se convierte en un campo de batalla y las armas son los programas, virus o aplicaciones informáticas. "Las tácticas de combate son la infiltración en redes enemigas, la recopilación de datos, la interferencia de señales inalámbricas, los programas informáticos falsificados y contaminados, ataques a sistemas enemigos a través de virus, gusanos y bombas lógicas, entre otras".[52]

Podría decirse que ciberguerra podría ser cualquier ciberataque pero no, se debe recordar que, al igual que en la guerra física, los enemigos tienen que ser los Estados. Si es posible el ciberataque de cualquier otro actor a un Estado pero esto no necesariamente involucra un acto de ciberguerra si no existe otro Estado que lo respalde, como en el caso mencionado de China y Estados Unidos.

Podemos agregar a la definición de ciberguerra[53] como una agresión "promovida por un Estado y dirigida a dañar gravemente las capacidades de

---

[50] *Ibíd.* p. 54

[51] Sain, Gustavo (2015); ¿Qué es la ciberguerra?, *Revista Pensamiento Penal*, (No. 10). p. 1-34

[52] *Ídem*

[53] En cualquier caso, la ciberguerra sigue siendo un conflicto asimétrico. Por ejemplo, una empresa también puede enfrentarse a un Estado o una empresa, a una organización civil o a civiles pero el que se considere ciberguerra dependerá de muchas cuestiones, empezando por el debate de lo que forma al término. La definición que ya tenemos de guerra: un conflicto entre Estados, por lo que la ciberguerra,

otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos".[54] Siendo esta agresión cada vez más sofisticada y complicada que ni la cuestión legal aún puede definir qué es, ni los Derechos tanto Humanos como de Estado al momento en que ocurre una agresión de este tipo.

Para poder establecer el concepto de ciberguerra debemos partir de la guerra física y los principios con los que se establece. El Derecho de Guerra es parte del Derecho Internacional que trata sobre la relación de los Estados en el momento en que se encuentran en un estado formal de guerra donde se llevan a cabo hostilidades reales en una guerra aun no declarada. Este Derecho está compuesto por normas ya establecidas en los tratados de diferentes convenciones a lo largo de la historia. Debido al creciente desarrollo tecnológico, la actualización de los instrumentos jurídicos es necesaria para comprender estos nuevos eventos, como lo es la ciberguerra.

Dentro de la guerra física, existen dos principios fundamentales que han ayudado a la creación tanto de Tratados o Convenciones Internacionales, como de prácticas de guerra y que hay que retomar pues serán aplicables a cualquier intento de ley o acuerdos sobre el ciberespacio. Estos dos principios son el *Ius ad Bellum* y el *Ius in Bello.* Ambos están plasmados en el Derecho Internacional tanto para la protección de civiles como la protección de la soberanía del Estado.

El *Ius ad Bellum* es un principio del Derecho Internacional que permite a un Estado el derecho de hacer la guerra. "Busca resolver los conflictos entre los Estados y busca legitimar las operaciones de guerra que se llevarán a cabo"[55]. Este principio fue planteado, en un primer momento, en el Pacto de la Sociedad de Naciones de 1919, luego en 1928 con el Tratado de París y ya se

---

entonces, al ocurrir en otro espacio debería ser considerada de la misma forma: un conflicto entre Estados. Pero debido al anonimato que el Ciberespacio te permite, es imposible tener una definición similar a la ya conocida. Por ello se tiene que analizar este concepto bajo otros términos y otras características.

[54] Sánchez Medero, Gema; La ciberguerra: los casos de Stuxnet y Anonymus; *Nueva Época*. (No. 11). España. p. 125

[55] Comité Internacional de la Cruz Roja (2010), Jus ad bellum y Jus in bello, *CICR*. Recuperado de: https://goo.gl/W8YdDL

establece como principio de guerra en la Carta de las Naciones Unidas de 1945, pero solo se acepta en caso de legítima defensa.

En cuanto al *Ius in Bello,* es un principio del Derecho Internacional que hace referencia a las prácticas aceptables mientras estás en guerra. Y sus disposiciones se aplican a todos las partes involucradas en el conflicto independientemente de las razones porque peleen. Tanto *Ius in Bello* como *Ius ad Bellum* se encuentran en el derecho internacional humanitario para limitar los sufrimientos provocados por la guerra. “En caso de conflicto armado internacional, a menudo resulta difícil determinar qué Estado es culpable de una violación de la Carta de las Naciones Unidas. Ahora bien, el sistema del derecho internacional humanitario no supedita su aplicación a la designación del culpable, pero si garantiza la protección de las víctimas de la guerra y de sus derechos fundamentales.”[56] Estos principios son necesarios para el derecho en cualquier tipo de conflicto.

El introducir la guerra al ciberespacio trajo cuestiones importantes al debate. El primero, los actores nuevos y la diferencia entre ellos. La segunda cuestión, la variedad de las armas cibernéticas y su multifuncionalidad”[57]. Los actores nuevos y el acceso y variedad de las ciberarmas han provocado discontinuidad en el debate sobre lo que se debe o no se debe hacer. Existen diferentes doctrinas que pretenden entender el uso de las armas cibernéticas según las funciones que han tenido cada una de ellas como se muestra en la siguiente tabla:

Tabla 4. Propuestas doctrinales de las armas cibernéticas	
Propuestas Doctrinales	**Descripción**
Autónoma	Es importante el instrumento. Es cuando el hardware y software se usan para hacer daño por el ciberespacio.
Concesiones finalistas	Efectos o consecuencias de la acción cibernética. Define el amar cibernética como el medio diseñado y usado para causar lesión o muerte en las personas o destrucción en las IC.
Concesión analógica	Equivalencia entre arma cibernética y física.

[56] *Ídem*

[57] Jornadas de Ciberdefensa 2016 Mando Conjunto de Ciberdefensa. Recuperado de: https://goo.gl/rpehcr

Tesis negacioncitas (*sic*)	No se puede calificar el arma cibernética porque no se puede calificar una acción cibernética como acción armada. No existe practica internacional que avale esa conclusión hasta que los efectos del arma cibernética fuesen más temporales que permanentes y más disruptivos que destructivos.
Concepto relativo	Cualquier objeto en realidad puede ser utilizado como un arma aunque no sea su intencionalidad previa.
Perspectiva funcional	El arma cibernética no es un objeto sino que se define funcionalmente como una acción por un sujeto determinado y un destino determinado con efectos concretos y con una intensión. Tiene el valor de reconocer la naturaleza polivalente de las acciones cibernéticas. Cada acción puede cumplir diversas funcionalidades.
Fuente: Robles Carrillo, Margarita (2016), Uso de la fuerza en el ciberespacio: las armas cibernéticas. Mando Conjunto de Ciberdefensa. *Jornadas de Ciberdefensa 2016* Recuperado de: https://goo.gl/rpehcr	

Respecto a los ciberataques, debido a que ha sido una evolución constante, gracias a sus características podemos destacar 3 formas de ciberataque, o ciberoperación similares a un ataque de guerra, como se aprecia a continuación:

Tabla 5: **Tipos de ciberataques que podrían considerarse para uso militar**	
Compute Network Operations (CNO)	
Compute Network Defense (CND)	Son acciones tomadas por el uso de redes de computadoras para analizar, proteger, supervisar, detectar y responder a la actividad no autorizada dentro de un sistema informático
Computer Network Attack (CNA)	Son medidas adoptadas a través del uso de las redes de computadora para interrumpir, negar, degradar o dar destruir a la información de las computadoras. Un ejemplo sería un *DDoS* o el Hacking orientado a sistemas para dejarlos fuera de servicio. El caso de Stuxnet es uno de ellos.
Computer Networl Explotation (CNE)	Son operaciones de apoyo y recolección de inteligencia, llevados a cabo a través de redes informáticas para recopilar datos del sistema enemigo.
Fuente: Gómez Arriagada, Héctor (2013). Ciberoperaciones. *REVISMAR*. Recuperado de: https://goo.gl/4gBLUm	

Imagen 5. Mapa de Ciberataques Kaspersky (28 de Septiembre de 2017)

KasperskyMap es una mapeo de los ciberataques y los tipos de ataque ciberataques en el mundo. Es creado por la empresa de seguridad Kaspersky. No es un rastreo exacto de los ciberataques pero si una aproximación de su origen y su destino. También puede conocerse el tipo de ciberataque más usado. Norse Corporation también cuenta con un rastreo de estos ciberataques.
Fuente: Kaspersky Lab. Cyberthreats Map. *Kaspersky.* Recuperado de: https://goo.gl/kNvWNh

Si se hace una comparación con las acciones clásicas, en la guerra física, podría decir que el *Computer Network Attack* sería el que más daños y prejuicios produciría a los Estados pues pretende atacar directamente a las personas y las Infraestructuras Críticas primordiales para el funcionamiento de un Estado. La legítima defensa de esta *ciberataque* estaría respaldada por el artículo 51 de la Carta de Naciones Unidas:

> Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales.[58]

El tema de la ciberguerra y los ciberataques tiene muchas cuestiones a considerar, en especial si se busca partir del concepto que ya se tiene en la guerra física y se busca reconfigurarlo al ciberespacio. Es necesario partir de los conceptos ya establecidos para poder reconstruir los elementos que componen dichos conceptos para que se adapten a estas nuevas situaciones que plantea el ciberespacio.

A nivel internacional no se han llegado acuerdos para comprender estos nuevos fenómenos, a nivel nacional si se podría hablar diferentes legislaciones, en diversos países, que se ven reflejadas en las estrategias nacionales de seguridad y defensa. La ciberseguridad comienza a ser parte de la seguridad de un Estado. La ciberguerra es un fenómeno que parte de estos métodos nuevos que implementa la ciberseguridad.

El anonimato, los nuevos virus informáticos, hackers, crackers, hacktivistas, ciberestrategia militar o espionaje industrial son solo algunos de los nuevos retos que vienen a transformar la concepción del ciberespacio. Tan solo ya la clasificación de ciberataques, como se muestra

[58] Naciones Unidas. Capítulo VII: Acción en caso de amenazas a la paz, quebrantamientos de paz o actos de agresión. *Carta de Naciones Unidas.* Recuperado de: https://goo.gl/c4ufSj

en la **Imagen 5**, son un primer riesgo. Es por ello que se necesitan implementar mecanismos que puedan transformar la dinámica mundial dentro este nuevo espacio. Es así como la ciberseguridad comienza a ser una pieza clave para el mundo tras todas las amenazas que este representa.

1.3.4 Sobre Ciberseguridad, Ciberdefensa y Ciberestrategia

El término *Ciberseguridad* puede definirse como "la aplicación de un proceso de análisis y gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información, datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados."[59] La ciberseguridad se ha convertido en un asunto prioritario para la agenda de los diferentes gobiernos pues las amenazas del Ciberespacio son cada vez más sofisticadas y de gran impacto para los Estados. Lo que se ha convertido en un gran problema debido a la pérdida económica y a los daños individuales que han producido.

La Ciberseguridad es otro término no definido de manera concreta pero bastante utilizada en documentos oficiales para hablar sobre las cuestiones que preocupan a los Estados en cuestiones de Ciberespacio. Antes que nada, se debe dejar en claro el otro tipo de amenazas que existen más allá de la ciberguerra y que son aún más comunes por lo que las estrategias de ciberseguridad se enfocan en estas cuestiones antes que en una legislación respecto a la ciberguerra, y se vuelve una parte importante de la Ciberdefensa.

La Ciberdefensa se transforma en un elemento prioritario de las Estrategias Nacionales. Puede considerarse como "la aplicación de medidas de seguridad para proteger los componentes de la Infraestructura Crítica contra ataques cibernéticos [además] de proteger la información procesada, almacenada o transmitida en los sistemas de información, comunicación u otros".[60] Existen diferentes tipos de amenazas que vulneran la Ciberdefensa de un país. Dependiendo de cada uno de ellos, se toman las medidas necesarias

[59] Ib*ídem*, p. 126

[60] Ministerio de Defensa (2012), El Ciberespacio. Nuevo escenario de confrontación. *Monografías del Centro de Estudios de la Defensa Nacional (CESEDEN)*. España. P. 211

para la aplicación de métodos que prevengan cualquier daño que puedan ocasionar tanto en las IC físicas como cibernéticas y dejar vulnerable a un Estado ante cualquier ataque. Los ejemplos en la siguiente tabla:

Tabla 6. Amenazas a la Ciberdefensa	
Tipo de amenaza	**Descripción**
Unidades cibernéticas de las Fuerzas Armadas Extranjeras (Ciberataque a Infraestructuras Críticas)	Ciberataque de las Fuerzas Armadas de un país extranjero a la Infraestructura Crítica de un Estado con el fin de perjudicarlo y obtener alguna ventaja de este incidente.
Servicios de inteligencia y contrainteligencia	Empleados por los Estados para realizar operaciones de información sensible o clasificada por los sistemas de información gubernamentales y de empresas nacionales de sectores estratégicos, incluso para el espionaje industrial.
Ciberespionaje Industrial	Es el robo de información a empresas con el fin de acceder a información como propiedad intelectual, desarrollos tecnológicos, estrategias de actuación, base de datos, etc.
Cibermercenarios	Grupo de hackers con conocimientos avanzados que son contratados para desarrollar ataques dirigidos contra un objetivo en concreto para obtener alguna información deseada
Ciberdelincuencia contra servicios financieros	Malware diseñados para el robo de datos de tarjetas de crédito, centrado en los dispositivos móviles. También son conocidos como Troyanos bancarios.
Ciberdelincuentes aislados	Se encarga de sustraer información de manera individual para después vender la información al mejor postor.
Ciberdelincuentes organizados	Mafias trasladadas al mundo virtual para cometer crímenes que ya han cometido en el mundo físico. Por ejemplo, fraude online, clonación de tarjetas de crédito, extorción, blanqueo de capitales, tráfico de armas, entre otros.
Ciberhacktivistas	Personas o grupos que, movidos por alguna ideología, intentan socavar la estructura del oponente. Un ejemplo muy conocido es Anonymus o Wikileaks.
Cibersabotaje	Se basa en encontrar los fallones en el acceso a sistemas de control mediante suplantación de la identidad digital.
Ciberterrorismo	Al igual que el terrorismo, su fin es generar terror o miedo generalizado en una población, clase dirigente o gobierno causando con ello una violación a la libre voluntad de las personas.
Fuente: Editorial (2014). Estas son las 10 ciberamenazas más comunes. *Periódico ABC*. Recuperado de: https://goo.gl/PJzGEi	

Pese a que existen muchas objeciones respecto a la militarización del Ciberespacio, hay otros que la defienden a partir de considerarla como un derecho de los países. De esta forma se dispone armamento en el Ciberespacio para la defensa de sus legítimos intereses. El pretexto siempre será el estar preparado frente a cualquier amenaza y siempre se buscará ser el más avanzado en cuestiones tecnológicas. Al final es posible que no se pueda evitar la militarización del ciberespacio aunque hay que tener en cuenta qué condicionantes pueden ocurrir.

Desde mucho antes que hubiera peligros respecto al Ciberespacio como los ataques a la IC, varios países ya estaban prestando atención a los asuntos como lo es el Plan de Acción de Ginebra en la Cumbre Mundial sobre la Sociedad de la Información de 2003. Esta Cumbre consistió en advertir los primeros retos de la Sociedad de la Información, sus vulnerabilidades y un primer acercamiento a una gobernanza en el Ciberespacio por parte de Naciones Unidas.

Esta Cumbre retoma temas prioritarios para las naciones, especialmente el de contar con una ciberestrategia nacional como un respaldo para las estrategias nacionales donde se protejan los sectores que implican más retos como las finanzas electrónicas, y en general se creen políticas que resguarden a las Tecnologías de la Información y Comunicación (TIC) de manera que puedan mostrar resultados para las naciones y sean fáciles de modificar según sean necesarias.

Tras el fin de la Guerra Fría, la noción de estrategia se transforma para las naciones en cuestiones de seguridad que implica “la preservación de sus valores esenciales, ausencia de amenazas y la formulación de objetivos políticos, su tema son los actores estatales y no estatales (organizaciones no gubernamentales y organizaciones intergubernamentales, entre otros)”.[61] Una estrategia maneja la discontinuidad potencial para trazar amenazas o presentar oportunidades.

Según las condiciones que se presenten, quieran o no sus participantes, muestran sus alcances. Es así como las circunstancias se juntan y pueden volverse en contra o a favor según la posición en la que se encuentre el

[61]Molina Mateos, José María (2014); Globalización, Ciberespacio y Estrategia Especial Consideración a la Estrategia de la Información, *Instituto Español de Estudios Estratégicos*, p.5

participante. Lo que hoy les favorece, al día siguiente, o quizá en unas horas o minutos, puede convertirse en una amenaza. Las decisiones correctas, o que aventajen en mayor medida, pueden marcar el destino de un país en situaciones críticas.

> La importancia de la estrategia radica, entre otras cosas, en la selección del esfuerzo político y militar en un escenario, de tal forma que logre una síntesis que permita resolver las cuestiones presentes, con clara visión de los escenarios futuros resultantes de las mismas. Lo que demanda un esfuerzo conjunto y multidisciplinar, caracterizado por la complejidad de elementos interrelacionados y por la incertidumbre de una amenaza no convencional, transnacional y sin respeto al Derecho Internacional [62]

En la actualidad, los desafíos de la seguridad son cada vez más sofisticados. El crecimiento de Internet en el mundo ha producido una gran dependencia a la tecnología que comienza a ser no solo una desventaja a nivel nacional sino también a nivel internacional. Esta visión nueva de la seguridad implica a nuevos actores, mucho de ellos de carácter no militar. Por ende, la seguridad ha pasado fronteras en cuanto a lo político y lo militar pues el Estado ya no tiene la capacidad de resolver cualquier amenaza por su cuenta y comienza a necesitar de otros Estados para la resolución de los conflictos.

La ciberseguridad necesita desarrollar una Ciberdefensa en donde se usen capacidades tanto militares como civiles, explotando los sistemas de información. Por ello, se crea una ciberestrategia a nivel regional, internacional y global que combata las amenazas del Ciberespacio. Esto ya es algo planteado para los espacios físicos, pues gracias al Ciberespacio, estos espacios también se ven vulnerados.

Un ejemplo de esto es la Unión Europea, esta cuenta con una defensa del Ciberespacio comunitaria con todos los socios de la UE y sus aliados donde se aseguran de que un país atacado pueda defenderse de los ataques cibernéticos y “se puedan tomar medidas contra los adversarios allá donde se encuentren. Para conseguirlo, ha de recurrir a los métodos clásicos de

[62] *Ibíd.,* p.10

cooperación entre Estados y abrirse a una colaboración internacional aún mayor".[63]

Pero esta defensa no existió de forma inmediata sino hasta varios años después de diferentes sucesos ocurridos dentro de la misma Unión Europea que dañaron sus Infraestructuras Críticas y a los civiles. La cooperación es necesaria para la UE, pues existen muchos puntos débiles, comenzando con que su ciberseguridad fue tomada como tema prioritario varios años después de que otros actores, como Estados Unidos, comenzarán a considerar al Ciberespacio un riesgo para la Seguridad Nacional[64]. O que su enfoque no es tan militar como lo es para Estados Unidos o Rusia.

Otros eventos internacionales corroboran la importancia de la ciberseguridad. La "Operación Octubre Rojo" fue un software utilizado, en 2007, para un ciberataque que permitía localizar y copiar documentos cifrados y no cifrados en determinados computadores. Este ataque tuvo cientos de víctimas, entre ellas se encontraban organizaciones diplomáticas, gubernamentales, de investigación científica, especialmente en Europa Oriental, Asia Central y otros países que pertenecieron a la disuelta Unión Soviética.

Se detectaron 300 computadores infectados, la mayoría de ellos pertenecían a embajadas, centros de investigación gubernamental, instalaciones aeroespaciales. La empresa Kaspersky "indicó que encontró 60 servidores de comando y control en Alemania y Rusia, que aparentemente eran controlados desde un sistema central que todavía no se ha podido encontrar."[65] Los países atacados pueden verse en el **mapa 5**.

Este malware se extendió por documentos Word, Excel, correos electrónicos, servidores de control y unidades USB. Aunque se confirmó que el software tenía un origen chino o ruso, lo único que se identificó correctamente fue que la información robada era de alto nivel, con datos geopolíticos de cada nación. Esto es un peligro debido a que la información puede ser vendida al mercado negro o a un país enemigo de la nación perjudicada. Denotando la importancia de incluir al Ciberespacio en la Estrategia Nacional.

---

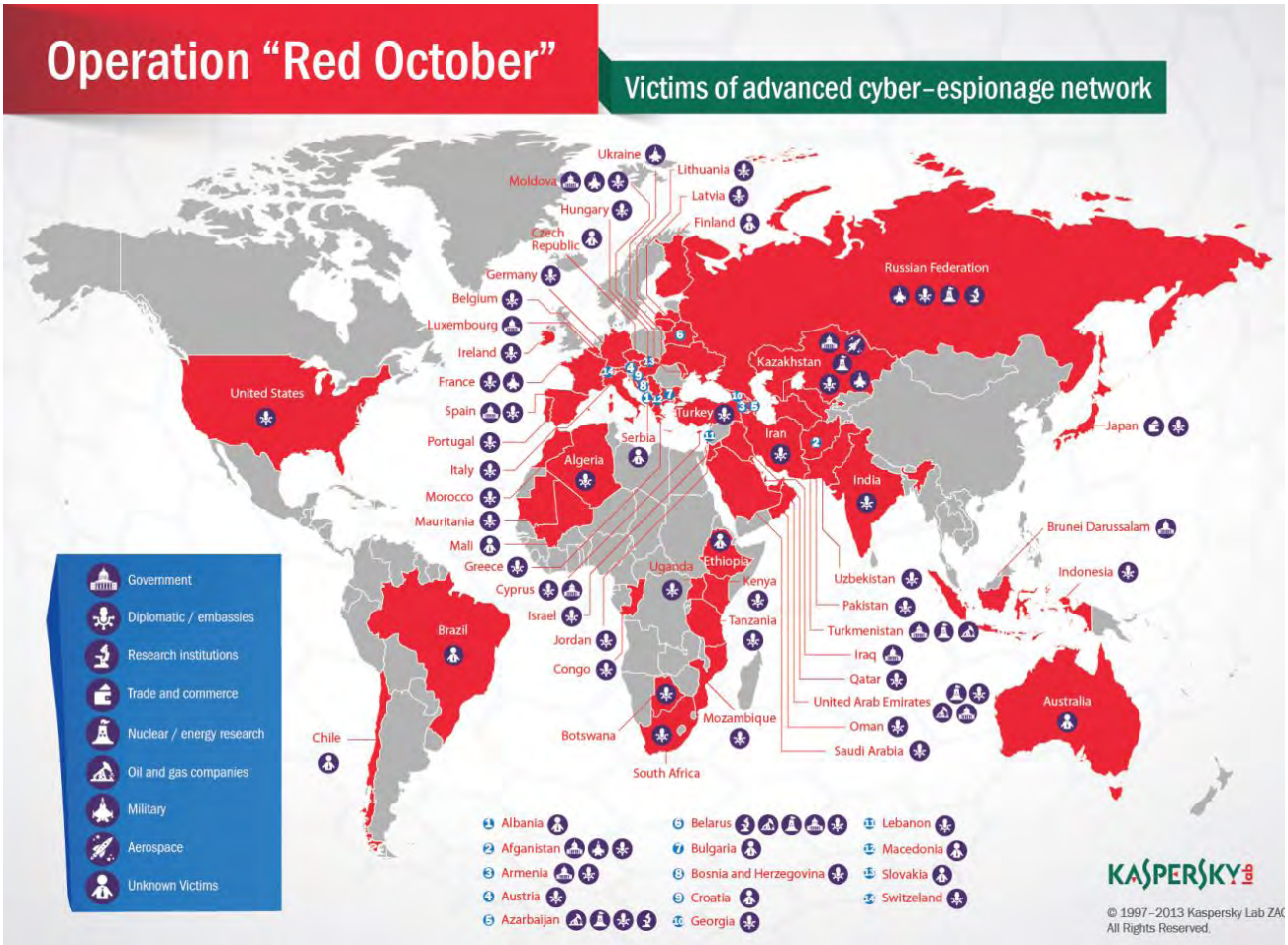
[63] *Ibíd.,* p.12

[64] En el capítulo 2 se hará una revisión más exhaustiva de la ciberseguridad en la UE.

[65] Sturm, Cony (2013). OperaciónOctubre Rojo: Es un nuevo ataque contra diplomáticos y organizaciones gubernamentales. *Fayer Wayer*. Recuperado de: https://goo.gl/ELSQkL

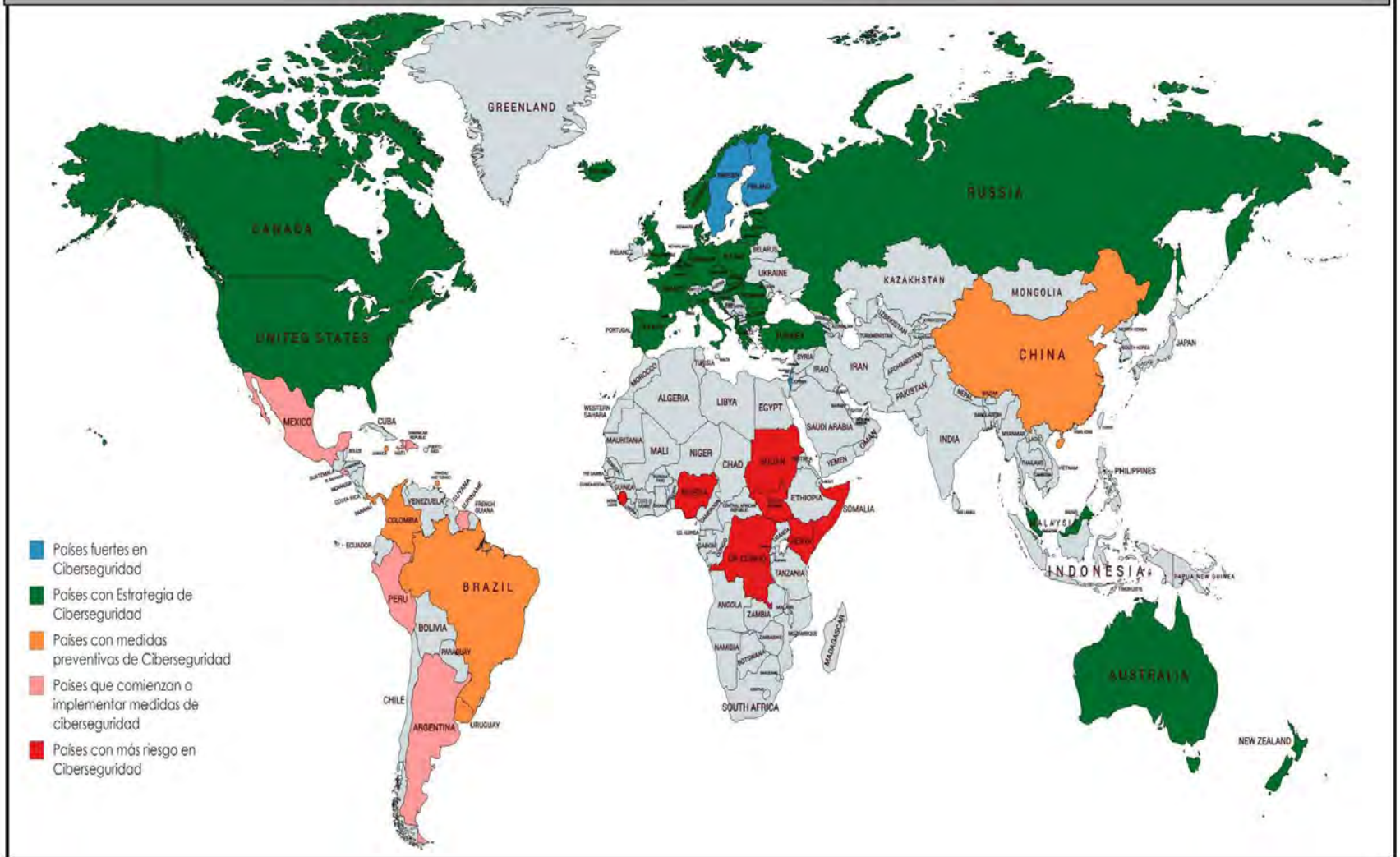
En el **mapa 6** podemos observar desde los países mejores preparados para los ciberataques masivos a los que menos lo están. El mapa nos da una idea de que la cuestión económica tiene que ver con la preparación de las estrategias de seguridad. Los países, donde apenas el internet comienza a llegar o a tener un auge más fuerte, realmente no se están preparados para delitos que naciones como Estados Unidos ya no considera tan peligrosos.

Mapa 5. Mapa de las Víctimas de la Operación Octubre Rojo



Fuente: Sturm, Cony (2013). Operación Octubre Rojo: Es un nuevo ataque contra diplomáticos y organizaciones gubernamentales. *Fayer Wayer*. Recuperado de: https://goo.gl/ELSQkL

Mapa 6. Mapa sobre la Ciberseguridad en el mundo



Elaboración Propia.

1.4 Teoría de la Globalización en un mundo interconectado

La globalización se ha convertido en una teoría para explicar al mundo y las transformaciones que ha tenido en los últimos años. La teoría de la globalización tiene el propósito de explicar todos estos acontecimientos y cómo ha cambiado el mundo para adaptarse. La teoría de la globalización se estudia a partir de 2 tendencias: los sistemas de comunicación y las condiciones económicas que promueven la movilidad de los recursos financieros y comerciales.

La teoría de la globalización señala que la estructura mundial y sus interrelaciones "son elementos claves para comprender los cambios que ocurren a nivel social, político, de división de la producción y de las condiciones particulares nacionales y regionales"[66]. La teoría comprende como premisa el hecho de que todo está integrado dentro y fuera de las sociedades, y estas a su vez juegan un papel primordial para las transformaciones.

El proceso de globalización comienza desde que se consolida el sistema capitalista como sistema económico dominante en el mundo. La desintegración de la Unión de Repúblicas Socialistas Soviéticas (URSS) y su sistema económico socialista empoderó al capitalismo como único sistema económico mundial. "La globalización implica un proceso de dominación de las poblaciones y de apropiación de las riquezas de vastas zonas del mundo por parte de los gobiernos de los países centrales y sus corporaciones privadas transnacionales".[67]

Existen temas que son prioritarios en la teoría de la globalización:

- La posición de los países como centro, semiperifería y periferia.
- Los patrones de las relaciones: relaciones pacíficas o de socios. Muchas veces su posición regional se ve influenciada la relación de estos.
- La diferencia económica de los países que pertenecen a la misma periferia. En muchas situaciones la diferencia económica es grande pese

[66]E. Reyes, Giovanni, *Teoría de la globalización: Bases fundamentales.* Siglo XXI. México. p. 44
[67]Batta Fonseca, Víctor; *Prospectiva y Teoría Internacional: Escenarios sobre el Estado y la Gobernabilidad en el siglo XXI*, UNAM, México, p. 32

a que pertenecen a la misma región. Un ejemplo de ello es Grecia, en la Unión Europea, siendo uno de los países más pobres de la región y con crisis económica pese a pertenecer a una comunidad que representa una potencia económica para el mundo.

- Las concentraciones económicas. "Estarían relacionados con los modelos de desarrollo dependiente".[68]

La llegada de Internet fue el primer paso para el desarrollo de la globalización debido a la reproducción de estructuras de poder, y el ya mencionado Ciberespacio. "El procesamiento de la información y de la comunicación (…) son el núcleo de esa transformación revolucionaria cuya esencia radica en la aplicación de ese conocimiento e información a aparatos de generación de conocimiento y procesamiento de información".[69]

Este mismo desarrollo ha sido tan veloz que tomar el control de estos asuntos ha sido lento por parte de los Estados. Los gobiernos no son capaces de adaptarse a los nuevos ritmos de actuación en la política, la normatividad y lo económico. En este último aspecto, se han creado nuevas posibilidades productivas pero la regulación de mercados se ha visto imposibilitada. Los nuevos actores mueven el mercado a su antojo dejando al Estado como un factor limitante. El control ya no está en un solo actor y se ha ingresado a un nuevo espacio: el Ciberespacio.

Sean Gallagher, investigador de la Universidad de Wisconsin, realizó un artículo sobre los posibles futuros del Ciberespacio denotando las debilidades y fortalezas del mismo.[70] Estos escenarios representan el impacto del Ciberespacio en el mundo y la interconexión del mismo. Algunos de ellos son:

- Technoutopismo: En este primer escenario, apunta que la ciberseguridad se vuelve más fuerte ante los cibercrimenes y a Las amenazas a la Infraestructura Crítica o la ciberguerra creando un

[68] E. Reyes, Giovanni, *Teoría de la globalización: Bases fundamentales*. Siglo XXI. México. p. 67

[69] Ibáñez, Josep, Globalización e Internet: poder y gobernanza en la sociedad de la información, en Batta Fonseca, Víctor; *Prospectiva y Teoría Internacional: Escenarios sobre el Estado y la Gobernabilidad en el siglo XXI*, UNAM, México, p. 78

[70] Gallagher, Sean (2015). Cybergeddon: Why the Internet could be the next "failed state". *ARS Technica.* Recuperado de: https://goo.gl/U5cfML

paraíso de seguridad en el Ciberespacio. En este escenario, la tecnología se basaría en la seguridad y habría una cooperación internacional al respecto. Podría decirse que es el escenario perfecto de acuerdo e interacción internacional con lo que refiere al ciberespacio. Todos los actores de la dinámica internacional están complacidos con lo que se ha logrado y existe cierta armonía.

- Status Quo: Existe la ciberdelincuencia y el ciberespionaje a altos niveles pero no existe la ciberguerra. La mayoría de empresas se preocupan por un ciberataque o fraudes en Internet pero hay algo de estabilidad y se toma en cuenta la nube[71] como un elemento para apoyo de la seguridad. Los Estados son quienes ayudan a cosificar la seguridad en el ciberespacio.
- Dominio de conflicto: El Ciberespacio se convierte en un campo de batalla. Cibercrimenes, ciberespionaje, o conflictos entre naciones están en todo el Ciberespacio. La ciberguerra podría ser una extensión de la guerra económica y las empresas se convierten en el "blanco suave" de los ataques políticos. El ciberespacio se puede convertir en un punto fundamental en las seguridades nacionales, en especial de países avanzados.
- Balcanización: No existe un solo Internet sino una colección de *Internets* nacionales que bloquean el contenido que no sea del mismo Internet nacional. Hay menos ataques directos y la seguridad solo le pertenece a los Estado nación. Se crean fronteras en el ciberespacio aunque, para realmente lograrlo, tendría que existir un mapeo total del mismo para poder comprender qué parte del ciberespacio puede pertenecer a un Estado y a otro. Podría decirse que el estudio de la ciberografía es primordial y ha formado parte de la comprensión del Estado para poder obtener este tipo de dominio sobre el ciberespacio.
- Cybergeddon: Es lo contrario al primer escenario: una distopía. El Ciberespacio no se puede gobernar, se convierte en una especie de "estado fallido". Todos los conflictos son posibles y los atacantes son

[71]La nube o nube informática es una forma de servicio que funciona a través de Internet que permite guardar información ya sea a nivel personal (de un usuario como música, fotos, videos) o a nivel empresa (se guarda la información más importante).

difíciles de controlar. Existe una brecha enorme entre seguridad o personas y los ataques más antiguos son los que más efecto llegan a tener. No existe control, ni uno moderado, y el ciberespacio se vuelve anárquico, como muchos activistas han querido pero este escenario es poco viable pues al final la infraestructura física del ciberespacio depende del control del Estado y si se convirtiera en un caos realmente sería cuestión de desconexión total.

La interconexión del mundo posibilita algunos de estos escenarios. El conflicto en este nuevo espacio existe y siempre habrá a menos que se halle un consenso internacional en donde se creen actores que controlen el Ciberespacio en su totalidad, lo cual es imposible o poco probable. Aunque la mayor parte del control recae en el Estado (como algunos países autoritarios, China por ejemplo), son los actores como empresas (tanto de Internet como físicas), hackers, crackers, grupos organizados, entre otros quienes llevan el verdadero control del Ciberespacio. Será un reto para los Estados imponer un control a este espacio para mantener en orden algunos problemas que hoy en día son bastante visibles.

La Unión Europea, ha buscado por años crear un Mercado Único Digital que conecte todas las economías pertenecientes a la UE y así lograr una mayor influencia a nivel internacional. Sin embargo, las amenazas a este plan son muchas, en especial cuando 28 economías-28 países-se convierten en una sola. Los problemas podría acrecentarse o podría existir un mayor control cuando 28 países están vigilando este único mercado. Esta iniciativa de la Unión Europea forma parte de lo que la globalización ha traído para el mundo: la necesidad de estar interconectados en todos los ámbitos.

Habría que comprender la evolución de la ciberseguridad de la Unión Europea para poder tener una perspectiva de lo que sería un escenario de esta magnitud. La posibilidad de diferentes escenarios es obvia pero se deben de comprender las iniciativas con respecto a la protección del Ciberespacio en la Comunidad Europea para saber qué tan viable podría ser una idea de Mercado Único Digital o que tan viable es constituir una estrategia fuerte de ciberseguridad para la comunidad europea.

Capítulo 2

La Unión Europea y los desafíos del ciberespacio

> *Para que el ciberespacio no deje de ser abierto y gratuito, deben aplicarse las mismas normas, los mismos principios y los mismos valores que rigen fuera de él en la UE. Debemos proteger los derechos fundamentales, la democracia y la primacía del Derecho en Internet. La UE está trabajando con sus socios internacionales, así como con la sociedad civil y el sector privado, para promover esos derechos desde una perspectiva global*
>
> *Catherine Ashton, Alta representante de la Unión en Asuntos Exteriores y Política de Seguridad, 7 de febrero de 2013, en la Comisión donde se publica la primera Estrategia de Ciberseguridad de la UE.*

Al comprender la importancia de ciberespacio y los cambios que ha traído para todo el mundo, se debe comprender cómo los sujetos internacionales han actuado para protegerse de las amenazas que conlleva estar conectado al mismo. En el caso de la Unión Europea (UE), las tecnologías de la información y la comunicación han representado una forma de integración tanto entre sus propios miembros como con terceros a lo largo de su historia. Sin embargo, la ciberseguridad en las políticas europeas ha tenido algunos tropiezos que si bien ha logrado superar, aún le queda un trabajo muy grande para poder establecer una ciberseguridad preparada para cualquier amenaza.

El inicio del desarrollo de la ciberseguridad de la UE comienza con las políticas en telecomunicaciones y la apertura del mercado en estas mismas. Las políticas de telecomunicaciones de la Unión Europea han transformado a los países miembros debido a la eliminación de monopolios nacionales que se habían establecido tanto por seguridad como por una política social e industrial. La apertura a nuevas competencia comerciales extranjeras ha enriquecido este sector.

La flexibilidad de las telecomunicaciones se debe a las exigencias impuestas en el mercado común europeo, la aparición de nuevas formas de transmisión (vía satélite e internet), los adelantos tecnológicos que modificaron el consumo de los usuarios (haciéndolos pasar de lo analógico a lo digital) y a

la necesidad de mejorar el sector económico de la unión atrayendo empresas extranjeras que cumplieran con las necesidades de la sociedad europea.

El desarrollo de servicios de telecomunicaciones, en especial los dedicados a Internet, fueron los elementos claves para el crecimiento de la economía a partir de implementar cierto tipo de empresas que dependen en su totalidad de la conexión ininterrumpida de Internet y la buena actividad de los sistemas de información. Desde los años de 1980[72] hasta ahora se ha visto una transformación inminente de la UE en este sector donde los acuerdos comerciales han sido parte de su crecimiento. La mayoría de estos acuerdos se han efectuado con empresas estadounidenses para el manejo de internet en sectores como los servicios de banca, servicios generales y constructoras[73].

La liberalización de las telecomunicaciones ha traído beneficios económicos a la UE. Estas reformas han colocado a la UE como un actor de gran relevancia internacional. Y aunque en un inicio esta liberación fue un enfrentamiento entre los monopolios nacionales y la apertura al libre mercado, hoy en día el beneficio ha sido tanto que ya se planea la creación de un solo mercado digital conformado por las 28 economías que componen a la Unión Europea.

La búsqueda del Mercado Único Digital permitiría "homogeneizar el ritmo de apertura y las condiciones competitivas de los Estados miembros a través del establecimiento de la "armonización" y alcanzar un equilibrio entre la imposición de la normativa supranacional común y el respecto al principio de subsidiariedad."[74] Igualmente, se debe comprender que por mucho que esta oportunidad comercial consiga beneficios a la UE, también traerá otros retos en los cuales la Comunidad europea no ha trabajado a profundidad. Esto hace referencia a toda la cuestión de la ciberseguridad.

Es hasta 2013 cuando se agregó la cuestión de Ciberseguridad como uno de los temas primordiales a tratar dentro de la Estrategia de Seguridad

[72] Cuando se comenzaron a crear las políticas en telecomunicaciones y que se eliminarían los monopolios nacionales, existieron muchos inversionistas preocupados por esta situación. En la actualidad, se han visto más los beneficios de la inversión extranjera en las telecomunicaciones de la unión en donde el objetivo actual es unificar los mercados digitales existentes en uno solo. Debido a la amplia oferta de empresas se necesita una renovación a las políticas comunitarias para la innovación digital y el control al respecto.

[73] *Cfr.* Ortiz, Carlos (2006). La Política europea en materia de telecomunicaciones: hacia la nueva sociedad de la información. Noticias Jurídicas. Recuperado de: https://goo.gl/5CNPYP

[74] *Ídem*

Europea. Pese a que el Consejo Europeo sí ha tratado algunos aspectos del ciberespacio, de ahí que se crearan instituciones encargadas de vigilar este sector, no ha existido un plan concreto para la prevención de amenazas. Y aunque sí se han explorado diferentes iniciativas que protejan los intereses de los miembros de la UE en el ciberespacio también han sido un reto a tratar. En especial en una economía que busca implantar un Mercado Único Digital, una acción que podría significar un gran riesgo para todos los actores que constituyen la UE.

2.1 Antecedentes sobre la Ciberseguridad la Unión Europea

En un primer momento, las prioridades para la Unión Europea siempre fueron de índole económica. La predilección de sus miembros fue buscar una estabilidad económica y así encaminar a la UE a ser uno de los actores más proactivos en la dinámica internacional. Cuatro etapas han representado la liberalización de las telecomunicaciones en la UE que a su vez nos pueden dar una idea de cómo se ha encaminado a la seguridad digital:

Tabla 7. Historia de las Normativas en Telecomunicaciones de la Unión Europea

Etapas	Años	Descripción
Monopolios	1984-1994	• En esta etapa se justificaban los monopolios de las grandes empresas. La preocupación estaba enfocada básicamente en la creación de un mercado comunitario de terminales. • Comienzan los primeros conflictos en Estados Unidos y Reino Unido acerca de la introducción de la libre competencia en el mercado de los servicios de telecomunicaciones • 1984- se adopta un acuerdo que apruebe un Plan de Telecomunicaciones donde se cree un mercado de terminales.
Libro Verde de las Telecomunicaciones	1989	• Habla del desarrollo del mercado común para servicios y equipos de telecomunicaciones supuso el inicio del proceso de liberalización del mercado de datos y servicios de valor añadido. En este mercado, la situación requería pasar de los operadores públicos nacionales, monopolísticos en sus respectivos países, a un entorno en el que cualquier agente del mercado pudiese operar en cualquier región comunitaria bajo unas mismas reglas del juego. • El modelo regulador desarrollado consistía en liberalizar las infraestructuras para que cualquier nuevo operador pudiera tener acceso a ellas en condiciones de igualdad. • El Libro Verde tiene dos principios fundamentales: -La armonización que refiere a las cuestiones técnicas de la normalización a la Oferta de Red Abierta.

		- La liberalización, que se refiere a la implantación de la competencia en los mercados de equipos y servicios. • El Libro Verde estableció algunas líneas de acción como: Mantener los derechos exclusivos de las administraciones en la explotación de la infraestructura de redes, todos los servicios deben ser liberalizados, interoperabilidad mediante estándares comunes, asegurar la introducción coordinada de la Red Digital de Servicios Integrados (RDSI), de las comunicaciones digitales móviles bajo el estándar GSM, el paging europeo y las Telecomunicaciones Inalámbricas Digitales Europeas (DECT por sus siglas en inglés).
Entorno Liberalizado	1995-1998	• Se adoptan mecanismos legislativos comunitarios básicos para alcanzar la liberalización plena del sector de las telecomunicaciones en 1998. • Se recogen 3 elementos fundamentales para la reforma: la abolición de los derechos exclusivos, la puesta en marcha de un nuevo marco regulatorio a nivel nacional y la creación de Autoridades Nacionales de Reglamentación autónomas e independientes. • El mercado más afectado por la regulación liberalizadora de este periodo es el mercado de telefonía fija. Aunque se logró liberalizar, los servicios aún se mantuvieron exclusivos por operadores públicos o dominantes. • El objetivo de esta reforma era garantizar la provisión de un servicio universal de telecomunicaciones, permitir acceso e interconexión a redes y servicios públicos de telecomunicación y garantizar la disponibilidad de un conjunto mínimo de servicios. • Para cumplir con su objetivo se armonizaban las condiciones para un acceso y una utilización abiertos y eficaces de las redes públicas de telefonía fija en el marco de un mercado abierto y competitivo y observando siempre los principios de la oferta de red abierta.
Nuevo Marco Normativo	1998-2000	• El progreso y la convergencia tecnológica, la innovación de la oferta de servicios, la rebaja de los precios y las mejoras de la calidad producidos por la introducción de la competencia en el sector de las telecomunicaciones han caracterizado este periodo y han constituido la base para la transición en Europa a la sociedad de la información. • Si bien los objetivos originarios fueron alcanzados, el proceso aún no ha sido concluido. La fragmentación del mercado comunitario frente a la mundialización de las tecnologías y los mercados, la dominación de los operadores históricos a pesar de la creciente competencia de los nuevos entrantes, la excesiva burocratización en un entorno dinámico, la velocidad sin precedentes en los avances tecnológicos y en el desarrollo de los mercados tradicionales y emergentes, han hecho necesario una revisión y puesta al día del marco regulatorio.
Fuente: Ortiz, Carlos (2006). La Política europea en materia de telecomunicaciones: hacia la nueva sociedad de la información. *Noticias Jurídicas*. Recuperado de: https://goo.gl/7Rb9BT		

El 30 de noviembre de 1999 se presenta ante el Consejo de Ministros de Telecomunicaciones la Comunicación *Hacia un nuevo marco para la infraestructura de comunicaciones electrónicas y los servicios asociados:*

revisión de 1999 del sector de las comunicaciones. “Esta Comunicación presentaba la necesidad de adaptar la normativa comunitaria de telecomunicaciones al mercado actual en competencia, recogía distintas propuestas de la Comisión sobre los diferentes aspectos del sector de las telecomunicaciones”.[75] Las directivas que se revisaron fueran sobre autorizaciones y licencias, servicio universal, acceso e interconexión y protección de datos en el sector de las telecomunicaciones, además de tomas de decisiones respecto al espectro radioeléctrico. Estas discusiones se basaron en cuatro principios políticos:

- Promover el mercado europeo abierto y competitivo para el servicio de comunicaciones mejorando los servicios ofrecidos al usuario.
- Garantizar el acceso asequible a un servicio universal especificado a escala europea. Además de establecer mecanismos de protección a los consumidores (Protección de datos e intimidad personal).
- Consolidar el mercado interno en un entorno convergente mediante la supresión de los obstáculos existentes a la oferta de redes y servicios de comunicaciones. Fomentando las construcción y desarrollo de redes transeuropeas.
- Salvaguardar los intereses comunitarios en las negociaciones internacionales y fomentar nuevos servicios a escala mundial.

Junto con estos fundamentos políticos también existieron principios normativos que se establecieron:

- Fomentar el empleo garantizando los objetivos de interés general cuando no sean satisfechos por las fuerzas de mercado.
- Reducir la regulación proponiendo una nueva cuando sea necesario por razones técnicas, económicas, de garantía de los ciudadanos o cuando el mercado sea incapaz de satisfacer unos objetivos particulares de interés público.
- Potenciar la autorregulación y la elaboración de códigos de conducta que reduzcan la regulación oficial.

[75] *Ídem*

- Asegurar la neutralidad tecnológica de manera que no se discrimine en favor de un uso particular.
- Alcanzar el consenso a escala mundial, regional o nacional.

Las acciones en telecomunicaciones explican por qué no se toman medidas de ciberseguridad que puedan prevenir cualquier incidente en el ciberespacio. El interés es mayormente en lo comercial. Se busca más una apertura de mercado que favorezca a la UE posicionándola como un actor de gran relevancia a nivel internacional. No se puede decir que la UE no le haya dado importancia a los ataques cibernéticos, pues ha construido planes de seguridad e instalaciones especializadas. La cuestión es que antes de 2013 no había concretado un plan de acción para la prevención de amenazas en el ciberespacio.

Para comenzar a explicar las acciones que siguieron en el nuevo milenio y nuevo siglo tenemos que explicar que la UE tuvo diferentes fases para concretar una política de ciberseguridad como la que se presenta en 2016, especialmente por todos los intereses de crecimiento económico a los que aspira. Fueron diferentes los elementos que llevaron a la actualización constante de la UE para establecer normas que pudieran vigilar las cuestiones del ciberespacio.

En un primero momento, es en el año 2000, cuando se publica un marco legislativo encargado del control del mercado electrónico, la información se encuentra en los **anexos 1, 2 y 3**. El mercado electrónico es parte importante de unas de las exigencias para esta apertura de mercado. Esta directiva lo único que buscaba era no vulnerar algunas reglas con las que se había establecido la UE y mantener la seguridad de datos de los usuarios. No había algo que previniera la vulnerabilidad que acarrearía una apertura de mercado de tal grado, solo la aplicación de leyes ya establecidas para la Unión Europea aplicadas al ciberespacio.

En el año 2000 se experimentaron diferentes problemas en las cuestiones de ciberespacio. Uno de ellos fue Reino Unido que sufrió 6000 ciberataques que provenían de Egipto, Pakistán, Marruecos y Turquía. O el virus ILOVEYOU, este virus provocó daños a casi todo país conectado en línea para ese año. Uno de los países afectados fue España, el 80% de sus

empresas sufrieron daños con pérdidas de aproximadamente 5 a 8 millones de dólares destinados a la eliminación del virus. En este momento la UE buscaba conectar a todos los miembros y modernizar todas sus funciones, era necesario considerar los peligros que esto también implicaba.

Tras los atentados de 2001, en Estados Unidos, el contexto de la seguridad, el mundo se transforma. La implementación de medidas de seguridad impuestas, por Estados Unidos, tenían que ser consideradas. La UE como actor que busca ser relevante para la dinámica internacional comienza a establecer medidas preventivas que apoyen las imposiciones de Estados Unidos sin alejarse de los intereses de sus economías. Podría decirse que la Unión Europea tuvo 3 fases iníciales que dan pie a la creación de una Estrategia de ciberseguridad como la que se presenta en 2013:

- La fase política: La comunicación sobre Seguridad de las Redes de la Información: Propuesta para una política europea. Esta exponía un primer antecedente sobre las obligaciones que debería tomar la UE respecto a las cuestiones de la criminalidad en el ciberespacio. Pese a lo prometedor de esta propuesta, no se deslinda de los planes económicos para modernizar la economía de la UE.
- La fase legal: Manteniendo los principios[76] con los que se crea la UE, se convoca al Convenio de Budapest sobre cibercriminalidad. Con este convenio la UE ya trata de desarrollar un marco legal para combatir esta cuestión no solo como actor bilateral sino a un nivel multilateral. El problema es sobre la forma en que se ha planteado el convenio y la falta de procedimientos contra infracciones. Además, su aplicación comienza hasta 2004 y aún tiene cuestiones a revisión.
- La fase de la seguridad: Esta parte es importante porque ya se habla sobre el ciberespacio en la Estrategia de Seguridad Común. La revisión de la Estrategia Europea de Seguridad de 2003 en 2008 plantea a la ciberseguridad ya como una necesidad para lograr los objetivos de la

[76] La UE en un principio se crea con base a manejar todas sus cuestiones en el ámbito político y legal. Como Unión no opta por ir a lo militar, pese a que algunos de sus miembros pertenecen a la OTAN. Y aunque es una relación diferente, muchas cuestiones de la OTAN intervienen en los acuerdos entre los miembros de la UE y retrasa muchos acuerdos o planes que buscan ser aplicados. Agregando los desacuerdos entre los miembros que no apoyan algunas iniciativas militares de la OTAN.

UE. Aquí ya no se habla de una resolución de problemas en el ciberespacio a nivel simplemente político o legal, sino de una cuestión que compete a la seguridad y tiene que ser tratada como tal, incluso una intervención militar. Pero de nuevo es muy poco lo que se puede rescatar de esta revisión. Son informes o revisiones posteriores lo que ya hacen un planteamiento más exhaustivo de la ciberseguridad.

El establecer una Estrategia de Ciberseguridad fue un camino largo a recorrer para la UE. Aún en 2016 sigue teniendo fallas al respecto pero las cuestiones del ciberespacio son relativamente nuevas. El internet trajo consigo un desarrollo tecnológico demasiado rápido y las legislaciones apenas logran acoplarse. Además, siendo la UE un actor relativamente nuevo y que experimenta todas las dificultades de contener 28 países pues las visiones no son las mismas y los desarrollos en cuestiones de seguridad tienen intereses encontrados.

Asimismo, la UE ha colocado en primer lugar la cuestión de una economía moderna que no permite crear un debate profundo respecto a todas las complicaciones que podría traer, por lo menos no lo hizo en un primer momento. La recopilación histórica de las fases que tuvo la UE para la creación de su Plan de ciberseguridad en 2013 muestran todas esas debilidades que no pudo resolver en su momento.

2.2 Seguridad de las Redes de Información: Propuesta para una política europea (2001)

El Consejo Europeo se reúne en Estocolmo, el 23 y 24 de marzo de 2001, para analizar y estudiar los avances económicos que ha tenido la UE en estos años. En especial para cumplir el objetivo acordado en Lisboa de ser un economía competitiva y la más dinámica del mundo. Entre los temas abordados fue envejecimiento de la población trabajadora; la creación de mejores empleos que aceleren la reforma económica y modernicen el modelo social europeo aprovechando las nuevas tecnologías; el mejoramiento de procedimientos para las siguientes reuniones y plantea procedimientos para cumplir la estrategia de Lisboa.

Se trazaron varias iniciativas y varios proyectos para la siguiente reunión de Gotemburgo que sería en junio de ese mismo año. Entre ellos estaba la cuestión de la seguridad de las redes electrónicas y de los sistemas de información. El Consejo pide a la Comisión la creación de una estrategia en materia de seguridad de redes electrónicas. En su mayor parte era por el crecimiento exponencial de los usuarios y el valor de las transacciones. La seguridad de la información busca implementar las innovaciones tecnológicas en la economía y colocar a la UE como un actor global importante.

La Seguridad de las redes electrónicas y los sistemas de información: propuesta para una política europea es el primer plan que da la UE para la constitución de políticas comunes con respecto a las cuestiones de ciberespacio. Debido a que se busca que todos los miembros de la UE estén conectados, las administraciones públicas comenzaron a revisar sus disposiciones en materia de seguridad. Y con el crecimiento de Internet, el compartir información valiosa ha aumentado por lo que también es considerado un punto vulnerable.

Los ciberataques en Reino Unido en 2000, por ejemplo, hicieron evidentes los efectos colaterales que un virus informático o ciberataque puede ocasionar. Este problema es más importante cuando todas las economías conectadas pueden verse afectadas. Internet es uno de los motores fundamentales en la productividad de las economías de la UE, por ello se busca crear un Plan en 2002[77] que busque comprender la situación de internet en la UE.

Esta propuesta política se divide en 2 parte, la primera es la definición de lo que es la seguridad de las redes de información:

> Las redes son sistemas de almacenamiento, procesamiento y transmisión de datos. Están compuestos de elementos de transmisión (cables, enlaces inalámbricos, satélites, en caminadores, pasarelas, conmutadores, etc.) y de servicios de apoyo (sistema de nombres de dominio incluidos en los servidores raíz, servicio de identificación de llamadas, servicios de autenticación, etc.).Conectadas a las redes existe un número cada vez mayor de aplicaciones (sistemas de entrega de correo electrónico, navegadores, etc.) y de equipos terminales (teléfono, ordenadores centrales, ordenadores personales, teléfonos móviles, organizadores

[77] Comisión Europea (2001); eEurope 2002:Impacto y prioridades; Estocolmo; Comisión Europea; recuperado de: https://goo.gl/wrcL1q

personales, aparatos electrodomésticos, máquinas industriales, etc.).[78]

También plantea los requisitos generales de seguridad que deben presentar las redes y sistemas de información. Estos son la disponibilidad, esto significa que los datos deben ser accesibles y debe tener servicios operativos en uso en cualquier tipo de alteración como catástrofes naturales o ciberataques; autenticación, confirmar la identidad del usuario y las entidades de gobierno o jurídicas a partir de procedimientos preestablecidos; integridad, confirmar el buen funcionamiento y manejo de datos; y confidencialidad, la protección tanto de los datos almacenados como de las comunicaciones. Se busca la protección de datos personales de forma eficiente.

Esta primera parte también plantea las amenazas en materia de seguridad a partir de la vulnerabilidad de las empresas y sus afecciones a la Seguridad Nacional de cada Estado miembro. Se hace un análisis por tipo de amenaza con el fin de crear un marco político para mejorar la seguridad de la UE. Los ataques más importantes mencionados son:

- Ataques contra los servidores de nombre de dominio: Para que internet funcione de forma correcta, el sistema de dominios debe funcionar de la misma manera pues es una simple traducción de códigos. Si estos fallan no se pueden localizar los sitios y podrían provocar un mal funcionamiento de la computadora. A una escala mayor podría provocar un desastre general al encontrar puntos débiles en los programas que contenían mayores servidores.[79]
- Ataques contra el sistema de encaminamiento: Busca crear *enrutadores*[80] que puedan determinar el destino del tráfico de datos. Ya que el internet es descentralizado, imponer *enrutadores* podría ser una buena forma para que ninguna información se vea vulnerada aunque existe el peligro de que puedan crear *enrutadores* alternos que modifiquen el destino del tráfico de datos.

[78] Comisión Europea (2001), Seguridad de las Redes de Información: Propuesta para un enfoque político europeo; *Unión Europea; Comité de las Regiones*, p. 5
[79] *Ibíd.,* p. 9
[80] También pueden conocerse como Bridge o puente de redes que conecta segmentos de red para lograr la conexión con otra y así lograr la transferencia del paquete de datos. Esto aplica para varias redes a su vez.

- Ataques por saturación y denegación de servicio: “Estas formas de ataque atentan contra la red sobrecargándola con mensajes artificiales que dificultan o impiden el acceso legítimo. Se podría comparar con el caso de un fax bloqueado por mensajes largos y repetidos. Los ataques por saturación tratan de sobrecargar los servidores Web o la capacidad de tratamiento de los proveedores de servicios de Internet por medio de mensajes generados automáticamente.”[81]

La primera parte también explora los nuevos desafíos que ha presentado la seguridad de la red y de la información. El principal es como todo este desarrollo ha transformado la vida económica y social de la sociedad. El segundo son los temas que podrían considerarse daños potenciales. Ambas tienen claro que el transporte de datos sensibles e información valiosa hacen un objetivo potencial de ataques a las personas, empresas o instituciones de gobierno. “La perturbación se puede producir a otra escala mucho más crítica, hasta plantear problemas como interferencias en las comunicaciones militares, graves cortes de corriente o importantes pérdidas comerciales debidas a ataques por denegación de servicio o de violaciones de la confidencialidad.”[82]

Ya que lo niveles de daños reales o potenciales no pueden evaluarse fácilmente por la deficiencia de la seguridad de las redes se tiene que disponer de un análisis profundo que vaya más allá de las experiencias anecdóticas y sus soluciones temporales que es lo que más se trabajaba en estos momentos respecto a la cuestión de seguridad en el ciberespacio.

La seguridad de redes tiene que avanzar a la velocidad de los cambios de las tecnologías, y esto representa un reto permanente. “Casi cada día aparecen en el mercado aplicaciones, servicios y productos nuevos. Pero es evidente que algunos factores del desarrollo de las redes suponen un importante desafío para una política de la seguridad privada y pública.”[83] Algunos de ellos son:

[81] Comisión Europea, Op. Cit., p. 5
[82] *Ibíd.,* p. 14
[83] *Ídem*

- Los objetos digitales que transitan en la red. Aquí se refiere a la cuestión de piratería. Mientras más objetos digitales existen, más fácil es el acceso a información a la cual se puede reproducir sin autorización.
- La limitación de redes IP que pueden moverse dentro de la red. Se necesitaría una identidad para poder accesar a este tráfico de red.
- Incrementará el uso de redes domésticas que conecta diferentes aparatos, esto podría crear amenazas que vulneren la seguridad de los usuarios. Además de todo lo que podría traer un "ambiente inteligente" que podrían crear debilidades en la arquitectura de seguridad.[84]

La segunda parte de esta propuesta de Seguridad de los Sistemas de Información, propone el enfoque político europeo. Este enfoque va dirigido a mejorar la seguridad de las redes y de la información. Esta propuesta es vista a partir del marco que existe sobre los servicios de comunicación electrónica, la protección de datos y la ciberdelincuencia. Esta parte hace un hincapié a que la protección de las redes debe importar en mayor medida a los responsables políticos para garantizar el funcionamiento adecuado de la economía. Muchas veces el problema reside en que el mercado no se ve interesado en intervenir en las cuestiones de seguridad y esto puede ser contraproducente.

> Se suele pensar que el juego del mercado equilibrará los costes del suministro de servicios de seguridad y la necesidad específica de seguridad. Algunos usuarios solicitarán mucha seguridad mientras que otros estarán satisfechos con un nivel menos alto de garantía, si bien el Estado podría garantizar un nivel mínimo de seguridad. Sus preferencias se reflejarán en el precio que estén dispuestos a pagar por los elementos de seguridad. No obstante, muchos riesgos de seguridad siguen sin estar resueltos o las soluciones a ciertos

[84] Por ejemplo, el *Internet de las Cosas*, que es todo lo que usamos de manera cotidiana y sea conectado al internet. La seguridad de nuestras casas, los aparatos cotidianos para limpieza, que en automático las ventanas se abran porque están programadas para abrirse cuando reciben cierto grado de luz (al amanecer). Podría considerarse algo similar al de las películas futuristas pero existen muchas implicaciones al respecto, empezando por todo el control que se tendría de nuestra vida cotidiana. Es comprensible que mientras se desarrolle la tecnología se busquen formas de facilitar la vida común de las personas pero esto mismo implicaría cuestiones como el control total de tu rutina. La rutina de una persona podría significar mucho porque no es solo la rutina de una persona, es de ciento de miles y si ya se han visto casos de vigilancia por parte de los gobiernos con la información que aportamos en las redes sociales, el conocimiento total de una vida podría implicar problemas a futuro. No todo progreso tecnológico nos beneficiaría a todos, y esto solo una cuestión del asunto. Los temas económicos o de seguridad nacional también sería parte del debate

> problemas de seguridad tardan en comercializarse precisamente debido a las deficiencias del funcionamiento del mercado.[85]

La mayoría de los ataques que se han logrado han sido a partir de usuarios no protegidos pues la inversión en mejorar la seguridad, de forma individual, muchas veces no es favorable para los usuarios o no lo consideran pertinente debido a los precios establecido por las empresas de seguridad. Aunque no toda la responsabilidad cabe en el usuario.

> Los usuarios no son plenamente conscientes de los riesgos en materia de seguridad y que muchos operadores, fabricantes y proveedores de servicios tienen dificultades para evaluar la existencia y difusión de vulnerabilidades. Muchos servicios, aplicaciones y programas nuevos ofrecen prestaciones atractivas que a menudo son fuente de nuevas vulnerabilidades. Si bien los beneficios son visibles, los riesgos no lo son y solo existen más incentivos para que los proveedores ofrezcan nuevas prestaciones en lugar de más seguridad.[86]

Internet fue creado para facilitar el acceso a la comunicación y el intercambio de datos, de tal manera su desarrollo ha sido favorable y efectivo. Desde este punto parte el problema pues es complicado tratar de proteger algo que no fue creado para ello. De ahí la importancia de la cooperación para trazar soluciones a la seguridad de las redes. Asimismo, es necesario crear un marco legal que deberá evolucionar según las necesidades que estas nuevas tecnologías vayan desarrollando.

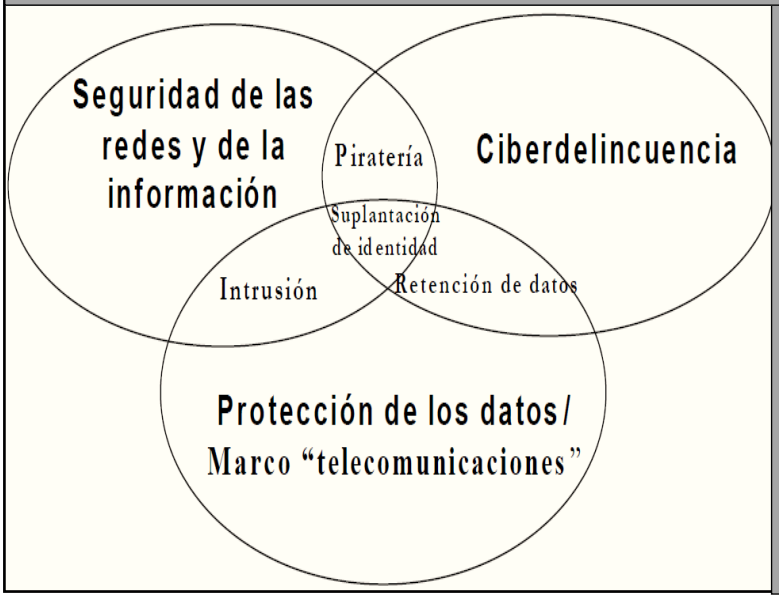
La creación de políticas de seguridad podría contribuir al "proceso del mercado y mejorar al mismo tiempo el funcionamiento del marco legal".[87] Algo importante en esta parte es la cuestión del Mercado Único Digital, si bien no es una mención tal cual, explica que el conectar todos los servicios de comunicación y de información transfronterizos en un solo mercado podría ayudar a la solución de estos problemas.[88]

Todas las intenciones plasmadas proyectan una UE desarrollada pero en esta primera fase solo se pueden tomar en cuenta las propuestas políticas en

[85] Comisión Europea, op. Cit. p. 13
[86] *Ibíd.* p. 15
[87] *Ídem*
[88] Aunque considero que esto podría ser contraproducente pues un solo mercado común que una todas las redes de las 28 economías, si es traspasada podría tener problemas realmente graves. Esto se analizará más a detalle en el 3er capítulo de la investigación.

telecomunicaciones y en protecciones de datos. Si menciona que el convenio de Budapest representa una primera etapa para la creación de un marco legal, pero como se verá en el siguiente apartado, no hay un marco legal aplicable inmediato y de hecho tarda cuatro años en ser aplicable.

Imagen 6. Interacción de las áreas que trabaja la Política de Seguridad de las Redes y la Información.



En el marco político de la UE es necesaria la aplicación de una política de seguridad de las redes y de la información.

Fuente: Comisión Europea (2001), Seguridad de las Redes de Información: Propuesta para un enfoque político europeo; *Unió Europea*; *Comité de las Regiones*, p. 17

Existen varios textos legales que pueden apoyar la cuestión de la seguridad en redes de comunicación pero todas son ideas dispersas y creadas para ciertos intereses. Han sido las Directivas sobre protección de datos las que han tenido más relevancia en estas cuestiones pero no garantizan un nivel de seguridad adecuado para los desarrollos tecnológicos y comunicación. Estas solo se basan en los intereses de los usuarios y las organizaciones, no a nivel UE.

Concluyendo con la propuesta, y como mayor reto a futuro, es necesaria la creación de un marco legal que realmente pueda actualizarse a la par que el desarrollo tecnológico de las comunicaciones. Para este primer año no tenía en cuenta el terrorismo como foco rojo de preocupación pues serían meses cuando ocurrirían los atentados en Estados Unidos. La UE ve primordial cuestiones básicas para la protección de sus intereses pero no desarrolló instrumentos sólidos que puedan responder a todas las necesidades

planteadas en la propuesta política, ni con el Convenio de Budapest sobre cibercriminalidad lo consigue.

2.3 Convenio de Budapest sobre la ciberdelincuencia (2001-2004)

Hablar del Convenio de Budapest sobre ciberdelincuencia es hablar sobre uno de los instrumentos internacionales que son antecedentes para la creación de estrategias nacionales. Este convenio es uno de los trabajos más importantes en el tema de la Unión Europea pues fue propuesto desde 2001 con intención de proteger a los usuarios en línea de cualquier tipo de delitos en el ciberespacio. Es en 2004 cuando entra en vigor, para 2005 y 2006 se unen más países, entre los más importantes se encuentran Estados Unidos.

El convenio trata de combatir delitos en internet como la infracción a derechos de autor, fraude informático, pornografía infantil, delitos de odio y violación a la seguridad de la red. Su principal objetivo es aplicar una política penal común que proteja a la sociedad contra el cibercrimen. Para ello, exhorta a buscar legislaciones adecuadas y fomentar la cooperación internacional.

> Convencidos de que el presente Convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tales como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación, sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable.[89]

El convenio comienza con los conceptos base para la comprensión del mismo. Estos conceptos representan una referencia de lo que podría representar dentro de las legislaciones nacionales. Los crímenes que se consideran dentro del convenio son:

- acceso ilícito
- interceptación ilícita
- ataque a la integridad de datos

[89] Consejo Europeo (2001); *Convenio de Budapest sobre la ciberdelincuencia*; Budapest; p. 13

- ataques a la integridad del sistema
- abuso de los dispositivos
- falsificación informática
- fraude informático
- los delitos relacionados con la pornografía infantil
- los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Se considera, dentro del Convenio, un tipo de acceso transfronterizo a los datos de informáticos para la asistencia mutua que puedan ser consultados por las partes, ya sea con consentimiento o que sea los que estén disponibles al público. Igualmente, busca la creación de una red 24/7 que garantice una asistencia rápida entre las Partes Colaboradoras. Al Convenio se le agrega un protocolo en donde también considerará delitos a la publicación de propaganda racista o xenófoba en las redes informáticas, y se buscaba incluir al terrorismo dentro de este Convenio aunque sigue siendo un debate.

El Convenio de Budapest tiene como objetivo la cooperación internacional entre Estados para combatir a la ciberdelincuencia que en establecer instrumentos legales que realmente las castiguen. Aunque se ha planteado la necesidad de unas reglas para determinar cómo se castigará cualquier delito, son solo algunas menciones al respecto.

Por ejemplo, en el artículo 22. Este artículo menciona que se considerarán infracciones a aquellos delitos cometidos en el territorio o a bordo de una nave que se encuentre sobrevolando el territorio de algún país. Al igual que aquellas sean ilegales aunque no pertenezca a este Estado o ningún otro. Pese a ello, no se especifica cómo se castigará tal delito. El castigo o lo legal quedan fuera del convenio, solo se dará apoyo a la intención del Estado a la hora de castigar.

Pese a sus problemas en estas especificaciones, la importancia de este convenio se puede explicar en el respaldo internacional que tuvo al momento de firmar, ratificar y aplicarlo. Fueron 54 países interesados que firmaron, 42 ratificaron y para 2014 eran 17 países que ya habían implementado el convenio en su derecho interno, se puede corroborar en el **anexo 4**. De igual forma, la participación de países no pertenecientes a la Unión Europea fue

bastante amplia, algunos de ellos fueron Costa Rica, Argentina, Chile y República Dominicana que ya han aplicado el convenio a su derecho interno.

La finalidad de este convenio, plasmada en el artículo 39, explica que este no busca ser una sustitución a los tratados internacionales de carácter bilateral o multilateral sino un complemento de los que ya existen para poder crear una normativa internacional que regule de mejor manera este aspecto. Y aunque la intención es un primer paso y busca trascender para crear tratados respecto a las amenazas que el ciberespacio conlleva, sus verdaderas intenciones no promueven una real solución al problema que representan los ciberdelitos.

Si un ciberdelito es cometido en otro Estado, estas malas conductas no serán castigadas de la misma forma que si fuese dentro del país de donde pertenece el cibercriminal. Muchas veces estos delitos ni siquiera son castigados o solo se dan pequeñas sanciones que no proceden. El convenio solo promueve la cooperación y pese a los años aún no se establecen castigos aplicables ni dentro de la UE ni a nivel internacional.

En el período que se mantuvo la discusión sobre lo que debería abarcar en el convenio (2001-2004) respecto a temas de ciberseguridad, había otros proyectos de la UE que buscaban encontrar aquellas debilidades y crear planes de acción que pudieran enriquecer todos estos mecanismos que querían implantarse tanto a nivel internacional, como a nivel UE. Uno de los factores que impidió un trabajo en esta área fue la guerra en Afganistán tras los atentados del 11 de septiembre de 2001 pues era inminente el apoyo que tenía que darse a Estados Unidos por parte de aquellos países pertenecientes a la OTAN (que en su mayoría son parte de la UE).

Es por ello que comienza, poco a poco, los estudios sobre las necesidades de los Estados miembros en el ciberespacio, aunque se hace más un estudio a lo que es Internet y las amenazas que trajo su implementación. Aunque hubo algunas iniciativas, era necesaria la creación de una institución que fuera la encargada de hacer todos estos análisis y crear recomendaciones para la protección tanto de las redes nacionales como las comunes.

2.4 Agencia de Seguridad de las Redes de la Información

Para 2002, el objetivo esencial era que todos los Estados miembros estuvieran conectados a internet. En este año se crea el plan de acción *eEurope*[90] 2002, agregado en los **anexos 5 y 6**, que tiene como fin la interacción efectiva entre los ciudadanos y la administración pública. Esta interacción se basará en tratar asuntos médicos, financieros, legales, entre otros, a través de internet. Para esto se busca desarrollar la cultura de la seguridad en los ciudadanos pues los datos a tratar serían delicados y personales. Es así como se busca adoptar, de forma obligatoria para 2002, las cinco directivas: marco general; el acceso y la interconexión; las autorizaciones y las licencias; el servicio universal y la protección de servicios de datos; y la competencia en los servicios de comunicaciones.

Para que todo funcione de una forma segura, cada miembro debe de incorporar requisitos básicos para poder llevar a cabo cualquiera de las actividades que se pretende. Entre uno de las medidas, la introducción de las firmas electrónicas para ofrecer servicios públicos es obligatoria, además de fortalecer los requisitos de seguridad en sistemas de información. El asunto de ciberseguridad en este punto solo se basa en la protección de datos sin profundizar demasiado en el asunto.

En 2003, se crear el reporte final de cómo funcionó el *eEurope2002* y los beneficios que se han traído a la UE. Y aunque muestra muchos beneficios, su idea es conseguir que la Comunidad Europea este totalmente conectada para poder agilizar muchas actividades tanto administrativas como de otras índoles. En este reporte también se tiene en cuenta que debido a que el sistema de salud comienza a funcionar con internet es posible que se convirtiera en una Infraestructura Crítica a futuro sin mencionar más al respecto. El siguiente reto es convertir a la sociedad de la UE en una Sociedad de la Información y ampliar el marco legislativo del comercio electrónico

[90] Los planes *eEurope* surgen con el objetivo de digitalizar a la Unión Europea. Cada cierto tiempo se crea un plan con ciertos objetivos para el crecimiento digital. Estos planes permiten conocer las formas de trabajo de la comunidad europea y los retos a trabajar en el siguiente plan. La primera vez que se plantean es en 2002 con el propósito de que la UE modernice sus servicios a los ciudadanos europeos.

Luego de que se creara la Estrategia de Seguridad Europea, en 2003[91], las prioridades se enfocan en el crecimiento económico europeo y la estabilidad de sus miembros, el tema del ciberespacio queda degradado a la cuestión de seguridad. Esto debido a que los planes de conectar a los miembros de la UE se centran más en las cuestiones económicas y políticas. Pese a todo ello, si comienzan a trabajar, de forma no tan prioritaria, las amenazas del ciberespacio. Para ello, la UE decide crear una agencia encargada de la protección de las redes de internet europeas.

En 2004, se crea la Agencia de Seguridad de las Redes y de la Información de la Unión Europea o *European Network and Information Security Agency* (ENISA). La ciberseguridad no es una prioridad en la estrategia común de seguridad, aun así se tiene en cuenta como un tema que podría ser alarmante, por ello la agencia es creada y comienza a trabajar de inmediato. Su primera misión es analizar la situación en la que se encuentran las redes de internet europeas.

Esta agencia es "un centro de conocimiento especializado en la seguridad cibernética en Europa. La ENISA ayuda a la UE y los países que la integran a estar mejor equipados y preparados para prevenir, detectar y dar respuesta a los problemas de seguridad de la información"[92]. La forma en que se apoya es ofreciendo soluciones a los problemas cibernéticos y asesoramientos de forma práctica para los sectores que lo requieran, ya sean públicos o privados mientras se encuentren en la UE. Este tipo de asesoramientos incluyen[93]:

- Organizar ejercicios de gestión de crisis cibernéticas a escala europea
- Contribuir al desarrollo de estrategias nacionales de ciberseguridad
- Fomentar la cooperación entre los equipos de respuesta a emergencias informáticas y la creación de capacidades

La importancia de la ENISA es la elaboración de políticas y legislaciones en la UE sobre seguridad en el ciberespacio. La colaboración con esta agencia

[91] Gazapo, Manuel (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista UNISCI*. (No. 43). p.62
[92] ENISA. Visión General. *Unión Europea*. Recuperado de: https://goo.gl/pP3oeu
[93] *Ídem.*

ha ayudado a la UE a crecer económicamente dentro de las ideas de liberalización de mercado. Pese a su creación, la importancia que se le dio no fue mucha. Las ciberamenazas eran constantes, especialmente en una red donde los datos de las personas navegaban a diestra y siniestra. La UE continuó con su idea de crecimiento económico dejando de lado la ciberseguridad mientras esta misma agencia comenzaba a estudiar los posibles problemas que una red desprotegida traería.

Al siguiente año, el ENISA publicó un reporte general de todo lo que se había hecho en el año respecto a la cuestión de redes de información. El General Report 2005 hacía un recuento de todo lo que había sucedido en el año desde la creación del ENISA, las juntas, los retos que estaban estudiando, las mejoras que se buscaba tener.

Al final, las perspectivas al futuro hablaban de[94]:

- Crear un Centro de Conocimientos especializados y de Excelencia en la Red y la Seguridad de la Información de la Comunidad.
- Protección a partir de la Seguridad de la Información
- Los beneficios traídos por la Sociedad de la Información y la Economía Digital fueron muchos por lo que se continuaría desarrollándolos y ampliarlos para el futuro
- Se tiene en cuenta el tipo de riesgos posibles que el internet puede tener como botnets, spam, malware, entre otros. Por ello se debe comenzar a prevenir cualquier ataque similar a los países miembro.
- El propósito del ENISA como un apoyo a toda la comunidad europea, asistencia al desarrollo de una ciberseguridad nacional que compete a cada gobierno y a las instituciones correspondientes. ENISA solo se encarga de dar soporte si es necesario o si es solicitado.

ENISA comienza a trabajar sobre la cuestión digital, de manera oportuna para comprender la situación digital propuesta en el plan *eEurope2005*. En este plan se muestra que la agencia ya ha comenzado a inmiscuirse dentro de las políticas digitales de la UE. El plan de 2005 busca desarrollar servicios,

[94] *Ídem.*

aplicaciones y contenidos, a la vez que permitir un acceso a Internet de banda ancha (alta velocidad). La UE no quiere que nadie se quede fuera de esta apertura digital. El plan es encontrar una forma de acceso viable para cualquier persona, ya sea que tenga una discapacidad, o la edad o alguna enfermedad no le permitan acceder a la red.

El plan *eEurope 2005* continúa con la línea del plan *eEurope 2002,* mantener los servicios públicos en línea de forma actualizada, promover el e-goverment (administración pública en línea), servicios de aprendizaje electrónico (eLearning), los servicios de salud también en línea, al igual que los negocios electrónicos y se agregará un punto importante: la infraestructura crítica tiene que mantenerse segura. De esta forma se puede adoptar otro tipo de instrumentos legislativos para mantener las prioridades. Para este año, un país que ya contaba con todos estos accesos era Estonia[95] quien ya funcionaba a través del e-goverment y casi todos sus sectores estaban en línea.

La revisión del plan 2005 permitió el reconocimiento de las debilidades que la UE tiene con respecto al ciberespacio. Por medio del intercambio de experiencias y aprendizajes entre los miembros se ha comprendido los retos que aún no han sido trabajados. Este plan percibió que internet y ciberespacio, en la agenda política, no han sido temas de gran interés o no se han considerado dentro de los temas principales a trabajar por parte de la Comunidad europea. Debido a ello, se crear la estrategia i2010, agregada en el **anexo 7**. Esta estrategia busca mejorar los planes *eEurope y* comprender aquellos temas que no son considerados como gran prioridad.

Esta estrategia plantea, por primera vez, crear un Mercado Único Digital. Agregando la importancia que le dará la UE en cuestiones de ciberseguridad. Es como lo económico sigue siendo el punto central de las estrategias a tomar por parte de la UE. Ahora que ya se cuenta con el apoyo de una agencia encargada de vigilar las cuestiones del ciberespacio, se proyecta un plan para tener redes seguras. Con redes seguras, la confianza de las personas crece al comprender que sus datos no serán robados o mal usados.

[95] De este caso se ampliará más en el tercer capítulo.

El elemento prioritario para la estrategia a seguir de la UE será a partir de la protección de datos personales (bancarios, médicos, comerciales, etc.) y así lograr que la UE se adentre a la protección de sus redes. El segundo elemento a proteger serán aquellas infraestructuras que dependan de la red y sean fáciles de vulnerar: Las Infraestructuras Críticas Europeas.

2.5 El libro verde sobre un Programa Europeo para la Protección de Infraestructura Crítica (PEPIC)

Las infraestructuras críticas, como se menciona en el capítulo anterior, son la parte fundamental para el funcionamiento de un Estado. Las IC son una conexión en el Estado para diferentes sectores. Dependerá del país para saber cuáles son las IC más importantes. El caso de la UE es un tanto peculiar debido a que existen dos tipos de IC: Las Infraestructuras Críticas Nacionales (las pertenecientes a cada país miembro de la UE) y las Infraestructuras Críticas Europeas (las que son compartidas con dos o más miembros de la UE).

Ya que la ciberseguridad es un tema relegado para la UE, ENISA fue el mejor elemento para acrecentar el interés en este sector. Tras su primer año de trabajo, ENISA ya detectó varios elementos vulnerables para la UE, entre los más destacados es la Infraestructura Crítica. Es así como busca promover mecanismos preventivos pues la fragilidad, y fácil vulnerabilidad, de las infraestructuras críticas se convierte en el centro de preocupación. En especial cuando varias IC son compartidas entre los miembros de la UE.

En 2004, Madrid, la capital de España, sufrió un atentado terrorista conocido como 11M. Este se dio contra cuatro trenes de la red de Cercanías de Madrid llevados a cabo por una célula terrorista de tipo yihadista[96]. Fueron 10 explosiones simultáneas en los cuatro trenes en la hora con más gente (en la mañana, entre 07:30-07:40). Fallecieron 193 personas y dos mil resultaron heridas. Estos atentados vulneraron la seguridad tanto del país como de la misma UE, por ello las Infraestructuras Críticas comienzan a ser ya un tema necesario a tratar en cualquier sector (comunicaciones, transporte, bancario,

[96]Yihadistas son aquellos que sostienen que el concepto del Yihad (Guerra contra el infiel) tiene legitimidad histórica y que acepta los llamamientos dictados por Alá. En la actualidad, el concepto es más utilizado para hacer referencia a aquellos radicales dentro del islam político.

etc.). La prioridad de la UE es mantener a sus miembros estables y los atentados terroristas comenzaban a ser un asunto serio para su seguridad como sujeto internacional.

En 2004, los atentados terroristas a Madrid dejaron en claro que cualquier daño a las IC podría ser perjudicial tanto para el Estado afectado como para otros miembros de la UE, en especial si compartes las IC. Junto con ENISA, el Consejo Europeo propone la creación del **Programa para la Prevención, preparación y respuesta de los ataques terroristas**.

El objetivo de este programa es que si llegase a existir un ataque terrorista, "la Unión Europea (UE) debe estar dispuesta a reaccionar y gestionar las consecuencias."[97] Para poder lograr el objetivo, la Comisión de las Comunidades Europeas (CCE-Comisión) establecerá ciertos mecanismos, instrumentos, propuestas para el combate del terrorismo. Al mismo tiempo, "la acción de la Comisión se referirá a los ámbitos de la protección civil y protección sanitaria pero también a la instauración de una red de sistemas de alerta que permitan una reacción rápida y eficaz en caso de ataque o accidente"[98]. Y desarrollará una conciencia de cooperación entre los estados miembros cuando sea requerido ese apoyo.

> En cuanto a la defensa de las infraestructuras críticas, la Unión Europea no cuenta con activos relevantes a la hora de proteger las infraestructuras empleadas durante la realización de misiones de la Política Común de Seguridad y Defensa (PCSD) que permitan una comunicación durante las operaciones desplegadas en entornos hostiles. El sector privado es un socio clave en el aprovisionamiento tanto vía satélite como línea fija terrestre o medios de comunicación móviles en este tipo de operaciones.[99]

El Programa es un inicio para poner en la mesa todos aquellos temas que no se les ha dado una importancia debida por parte del Consejo Europeo, y en general de la Comunidad europea. Las preocupaciones por avanzar en la seguridad de los miembros son fundamentales. Y desde los primeros ataques terroristas, las IC se volvieron el blanco fácil y lo más difícil de proteger.

---

[97] Comisión de las Comunidades Europeas (2004). *Comunicación de la Comisión al Consejo y al Parlamento Europeo: Prevención, preparación y respuesta a los ataques terroristas.* Bruselas. Pag. 3

[98] Ibíd., p. 6

[99] Comisión de las Comunidades Europeas (2005). *Libro Verde sobre un programa europeo para la protección de infraestructuras críticas.* Bruselas. Pag. 7

En julio de 2005, en Londres, Inglaterra, ocurren cuatro explosiones en el sistema de transporte. Tres son en el metro de Londres y la cuarta en un autobús urbano. Las explosiones en el metro produjeron un saldo de 700 muertos mientras que la del autobús provocó 56 muertos, entre ellos los terroristas. Se le dio la autoría del atentado a Al Qaeda. Esto implantó un sentido de urgencia a la seguridad de las IC, más allá del Programa contra el Terrorismo.

El Consejo Europeo insiste a la Comisión a crear una estrategia global[100] que proteja las IC. La Comisión propone la creación de un **Programa europeo para la protección de infraestructura crítica (PEPIC).** Para ello crea la Comisión de una Red de Información sobre alertas en infraestructuras críticas (CIWIN) y esta organiza dos seminarios para crear un debate entre los Estados miembro sobre este tema. Junto con el apoyo de ENISA, los seminarios empiezan de inmediato.

En el primer seminario se crean propuestas por parte de los Estados miembro sobre lo que consideran una IC. Para el segundo seminario, se contó con la participación de asociaciones competentes de cada sector, además de los Estados miembros. Tras este análisis se presenta el **Libro Verde sobre un Programa Europeo para la protección de infraestructura crítica (noviembre de 2005).** Este libro Verde explora los peligros de las IC que van más allá del terrorismo, como lo son: catástrofes naturales, actividades delictivas, acciones malintencionadas, entre otros.

> El principal objetivo del Libro Verde es recabar puntos de vista en torno a las posibles opciones para el PEPIC gracias a una amplia participación de los agentes interesados. Una protección eficaz de las infraestructuras críticas requiere la comunicación, coordinación y cooperación, en el ámbito tanto nacional como de la UE, entre todas las partes interesadas: propietarios y operadores de infraestructuras, reguladores, asociaciones profesionales y empresariales en cooperación con todos los niveles de la administración y el público en general.
>
> El Libro Verde presenta las opciones para una respuesta de la Comisión a la solicitud del Consejo de establecer el PEPIC que constituye la segunda fase del proceso de consulta con vistas al Programa europeo de protección de infraestructuras críticas. Una vez presentado el Libro Verde, la Comisión espera recibir propuestas concretas sobre las opciones que en él se exponen. En función del

[100] Cuando hace referencia a global, es debido a que quiere competer a todos los miembros

> resultado del proceso de consulta, el conjunto de medidas que integren el Programa podría presentarse en 2006.[101]

El análisis que se logró con el Libro Verde, planteó el propósito que tendría el PEPIC de manera global. Este se encargaría de asegurar "los niveles adecuados y equivalentes de seguridad en las infraestructuras críticas, minimizar los puntos de fallo y proponer mecanismos rápidos y probados de recuperación de infraestructuras para toda la Unión"[102]. Estos niveles de protección variarán según el tipo de IC pues depende del daño que pueda ocasionar su falla. Estos procesos serán permanentes, se harán revisiones constantes o si surgen inconvenientes.

Este programa está encargado de reducir al mínimo cualquier impacto que pueda presentarse, de forma negativa, en cualquier sector. Además de calcular los costes que pudieran afectar la estabilidad de los mercados como la evaluación en el mercado de valores. El libro verde plantea que se deben mantener 3 planteamientos importantes:

- Un planteamiento global frente a todos los peligros: este buscará atender a las amenazas tanto intencionadas como los catástrofes naturales, así como cualquier otra amenaza posible sin considerar el terrorismo.
- Un planteamiento global con prioridad sobre terrorismo: atenderá otros peligros que surjan de amenazas intencionadas o catástrofes naturales pero teniendo en cuenta un posible ataque terrorista.
- Un planteamiento centrado en la amenaza del terrorismo: Este solo se centrará en el terrorismo, en ninguna otra amenaza más.

Estos planteamientos se basarán en los siguientes principios:

- Subsidiariedad: La protección de IC será responsabilidad nacional. En cuanto a las IC transfronterizas competerán a la Comisión. Cada uno adoptará las decisiones y planes que mejor crea para proteger sus activos.

[101] Comisión de las Comunidades Europeas Op. Cit. Pag. 3
[102] *Ídem*.

- Complementariedad: Las medidas ya existentes tendrán que seguirse al pie a menos que existan mecanismos comunitarios diferentes.
- Confidencialidad: la información compartida sobre la protección de IC será de confianza y confidencialidad con el objetivo de mantener su seguridad.
- Cooperación de los agentes interesados: Cualquier agente interesado (Estados miembro, la Comisión, las asociaciones sectoriales o profesionales, etc) deben desempeñar un papel de protección a las IC. Cooperarán para la protección de las IC según las funciones que les competan.
- Proporcionalidad: Las medidas y estrategias de protección dependerán del grado de importancia o las consecuencias posibles. No todas las IC pueden ocasionar los mismos daños.

Las nuevas tecnologías (internet) y la liberalización de mercados son una amenaza ya confirmada en este estudio. Debido a que la liberalización de mercados es prioridad para la UE, busca crear marcos legales que le permitan continuar con esta liberalización sin perjudicarse a sí misma. Las medidas de protección común son un primer inicio. La Comisión buscará facilitar la definición, intercambió y difusión para que se lleven a cabo las mejores prácticas aunque no todos los Estados se verán obligados a cooperar a menos que así sea establecido.

Ahora, las IC son un tema bastante complejo, más en la UE. Como se mencionó, las Infraestructuras Críticas Europeas (ICE) se dividen en dos, las nacionales y las multilaterales. Ambas tendrán diferentes enfoques en el Programa debido a que son diferentes los encargados de su protección, como se mencionó antes. Se considera bilateral cuando sus efectos son transfronterizos y pueden repercutir fuera del territorio donde se encuentran instaladas. Estas competen a dos o más Estados miembros aunque no implica que sea necesaria una mayor protección, todo se medirá según el nivel de impacto. A estas se les llamará Infraestructuras Críticas Europeas (ICE) y serán asunto tanto de los Estado miembro, la Comisión y operadores que competan a casa una de ellas.

En cuanto a las Infraestructuras Críticas Nacionales (INC), cada miembro se hará cargo de su protección. Ya sea que se cree un organismo especializado o alguna organización sin autoridad. El papel de las ICN fue difícil de admitir pues debido a que la propuesta del Programa pretende ser global y no nacional, las ICN podría haberse excluido del programa pero al final serán una forma de consideración obligatoria para los Estados miembros.

La complejidad de este tema en la UE no solo se queda en la diferencia entre ICE o INC sino en saber a quién pertenecen (más allá del Estado o Estados miembro). Con la apertura de mercado, no es difícil que varias empresas sean las dueñas o las mayores inversoras en IC importantes a nivel nacional o a nivel europeo. Este es un elemento que también hay que considerar pues sin la estrecha cooperación con las empresas, es muy difícil que crear una estrategia de protección segura, además de que se podrían convertir en una amenaza para el Estado.

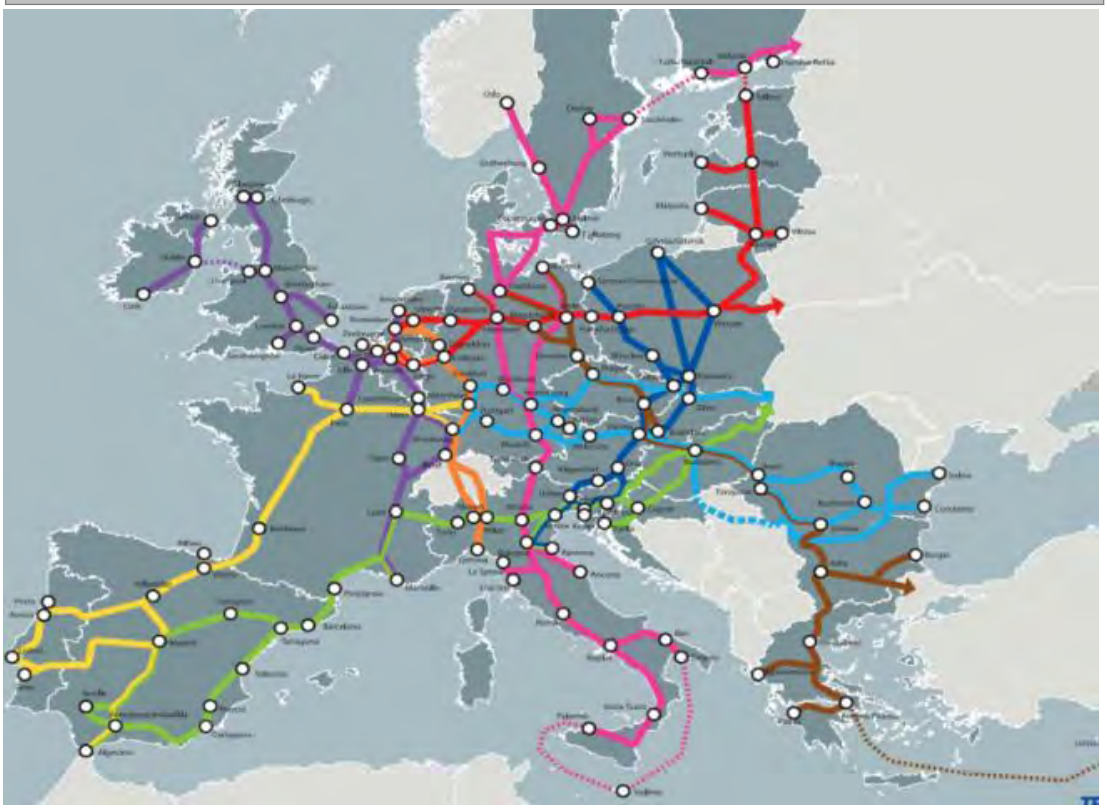
El ejemplo de esto podrían ser las empresas de gas en la Unión Europea. Se convierte una campaña campal saber quién será el mayor distribuidor de gas en la UE y debido a la necesidad del gas, Europa tiene que mantener márgenes de protección si llegase a ser escaso o si solo una empresa llegará a ser la única distribuidora de gas. Como ocurrió la adhesión de Crimea a Rusia. Fue parte de la estrategia política contra Europa y trajo problemas con el suministro de gas debido al aumento de precios por parte de Rusia. Y siendo el gas ruso del que más depende la UE, sería un problema grave a solventar pues afectaría a una ICE y sus empresas dependientes del gas.

Aunque este no es un hecho que compete a la investigación, ilustra la importancia de las ICE y la necesidad de una cooperación para coordinar la seguridad de las ICE. El carácter privado debe ser un elemento importante en la cuestión de ciberseguridad debido a que existen cada vez más empresas que se adueñan de las IC más importantes de un Estado, y en el caso de la UE las IC compartidas son un punto de riesgo importante[103].

[103]En este punto ¿quién debería de proteger la IC privada? ¿La empresa o el Estado? Aunque es recomendable una cooperación a la seguridad, hay IC que no tienen un impacto fuerte para el Estado y son de carácter privado, además de que la empresa es la que muchas veces está mejor preparada para cualquier problema que esta IC presente. Se deben de comprender estos elementos en la prevención de

El Consejo Europeo aprueba el PEPIC a finales de 2006 para comenzar con la aplicación del Programa. Este sería una de las tantas bases que la UE necesitaba para poder comprender los problemas que tiene con su ciberseguridad. El convenio de Budapest, el ENISA o el Libro Verde sí han promovido la cooperación tanto internacional como entre los mismos miembros pero eso no será lo único que se necesite para poder detener las amenazas. Se necesita un análisis exhaustivo para comprender los retos que aún tienen la UE por resolver.

Imagen 7. Ejemplo de Infraestructura Europea: Red de trasporte Transeuropeo



Ejemplo de lo que podría ser una infraestructura bilateral o multilateral. Las ICE son definidas por los miembros de la UE y la Comisión por lo que queda a su criterio cuales son las más importantes. Una red de transporte podría representar una ICE pues involucra a varias partes.

Fuente: European Comission. Infraestructure-TEN-T-Connecting Europe. *Mobility and Transport.* Recuperado de: https://goo.gl/GEChZL

problemas y la creación programas para la seguridad. Y aún más cuando muchas de estas a comienzan a ser parte del ciberespacio.

Imagen 8. Ejemplo de Infraestructura nacional: Red de carreteras alemanas

Las ICN son definidas por el mismo miembro de la UE según la importancia.

Fuente: Mapa Carreteras (2016). Guía de caminos y carreteras en Alemania. Recuperado de: https://goo.gl/Zay2kH

2.6 Revisión de la Estrategia Europea de Seguridad de 2003 en 2008

La Estrategia Europea de Seguridad de 2003 representó un gran paso para la construcción de la política exterior y de seguridad de la Unión Europea. Propone por primera vez, puntos en el que todos los miembros tenían un acuerdo para evaluar y comprender las amenazas a su seguridad en conjunto. Esto también incitó a la propuesta de objetivos comunes de seguridad. En su momento fue llamada como Estrategia para *Una Europa Segura en un mundo mejor* buscando plasmar las aspiraciones idóneas de la UE.

La Estrategia Europea de Seguridad fue redactada por instancia del Alto Representante de la UE para la Política Exterior y de Seguridad Común: Javier Solana, en ese momento. Esta definía los principales retos a nivel mundial y las principales amenazas contra la UE. Esta Estrategia planteó objetivos a seguir para combatir estas amenazas.

El tener a Estados Unidos como modelo para la creación de esta Estrategia Europea de seguridad era un poco caótico debido a que la UE es un actor multilateral, representa a varios países, a diferencia de Estados Unidos que se representa a sí mismo y sus intereses. Las ideas e intereses de los Estados miembros, la Comisión y el Consejo chocaban al momento de establecer mecanismos de aplicación. En el caso de los Estados miembros, pese a ser un conjunto, al final cada Estado miembro era responsable mismo de su propia Seguridad Nacional por lo que las visiones chocaban bastante al momento de establecer estrategias o políticas que puedan competer a todos.

Otra cuestión es la rendición de cuentas, los Estados miembros solo rinden cuentas en Seguridad a los ciudadanos de su país y los parlamentos nacionales. La UE solo dispone del ejercicio de competencia que recomienden sus Estados miembros y estos no responden sus actos de Seguridad ni ante el Parlamento Europeo ni ante los ciudadanos europeos (no nacionales). Y por último, el interés de la UE por ser un actor global influyente choca con la forma en que plantea su Política Exterior.

> Cualquier actor que aspire a ser global debe enmarcar su estrategia de seguridad en una estrategia de acción exterior, lo que se conoce como grandstrategy, donde se recogen los grandes principios, valores y patrones de comportamiento en su actuación internacional. Esto no ocurre en la UE y se da la paradoja de que estando la

> Política Europea de Seguridad y Defensa (PESD) subordinada a la Política Exterior y de Seguridad Común (PESC), la PESC no cuenta una estrategia de orientación y la PESD sí.[104]

Hay que tener en cuenta que la UE es un actor que para ese momento recién construye sus bases. El tener a Estados Unidos como ejemplo para construir su Seguridad y Defensa es debido a todo el desarrollo que ha tenido en este tema, en cambio la UE es un actor que recién comienza y es aún más complejo porque no solo está viendo por los intereses de una parte sino de un conjunto de países con ideas totalmente diferentes e intereses que muchas veces no concuerdan.

No todo es malo para esta Estrategia pues en un primer momento rompe con la idea civil en la que se construyó la UE. La UE se construye como una comunidad política basada en el derecho para integrar a los Estados y pueblos Europeos. Aunque sus primeros acuerdos eran estratégicos con respecto a los recursos como acero y carbón, el resto de su constitución siguió siendo política sin involucrar cuestiones de seguridad más allá del derecho o acuerdos internacionales.[105] La Estrategia Europea de Seguridad representa un primer paso para que la UE se muestre activa y cooperativa respecto a las cuestiones de seguridad a nivel internacional: aportar más recursos, mejor gestión con los miembros y una actuación inmediata.

En la acción, existieron muchas ideas contrarias con respecto a las decisiones que se estaban llevando. El alegato de que la decisión del uso de la fuerza es solo de los Estados, las diferencias en las estrategias nacionales o el que no se deja en claro la forma en que será usada la fuerza militar. Aunque la Estrategia no está del todo establecida, sí confiere obligaciones a la UE como las amenazas inminentes que tiene que combatir la UE. Entre ellos podemos mencionar:

[104] Arteaga, Félix; La Estrategia Europea de Seguridad, cinco años después*;* Real Instituto El Cano Royal Institute; España, Recuperado de: http://bit.ly/2nHUwPr

[105] La cuestión con la OTAN es diferente porque no todos los países de la UE pertenecen a la OTAN. Aquí solo hago referencia a las cuestiones militares o de seguridad dentro de los acuerdos de la UE, no considero la pertenencia a ningún otro organismo internacional.

- Proliferación de armas de destrucción masiva
- Terrorismo y delincuencia organizada
- Seguridad Energética

Aunque esta estrategia representó un gran cambio para la Seguridad Exterior Europea, fue hasta 2008 que se consideró el actualizarla pues no se estableció una periodicidad para su actualización como las estrategias nacionales. El informe no buscaba renovar la estrategia, solo evaluar los resultados de los últimos 5 años. Así mismo, agregar aquellos temas que no han sido prioridad para la UE presentando algunas líneas de acción. El informe que se presentó fue *Ofrecer seguridad en un mundo en evolución* en la que se examinaron los fallos y las faltas de esta Estrategia y fue donde se consideraron, como temas relevantes para toda la Comunidad Europea, los temas de Ciberseguridad y Cambio Climático[106].

Sobre la Ciberseguridad:

> Las economías modernas dependen en gran medida de las infraestructuras vitales como los transportes, las comunicaciones y el suministro de energía, e igualmente de internet. La Estrategia de la UE para una sociedad de la información segura en Europa, adoptada en 2006, hace referencia a la delincuencia basada en internet. Sin embargo, los ataques contra sistemas de TI privadas o gubernamentales en los Estados miembros de la UE han dado una nueva dimensión a este problema, en calidad de posible nueva arma económica, política y militar. Se debe seguir trabajando en este campo para estudiar un planteamiento general de la UE, concienciar a las personas e intensificar la cooperación internacional.[107]

La ciberdelincuencia y terrorismo eran elementos importantes a tratar para la UE. Todo esto tras los ataques a las IC tanto privadas como gubernamentales de algunos Estados Miembro. En especial la ciberdelincuencia, ya fue tomada como un arma que podría afectar tanto económica, militar y políticamente. El informe hace hincapié en la necesidad

[106] Sobre el Cambio Climático hace una recopilación de los Informes que han trabajado este tema. De igual forma habla de los posibles problemas que podrían existir sobre las rutas comerciales, las zonas marítimas y los recursos que anteriormente eran inaccesibles.

[107] Secretaría del Consejo de la Unión Europea (2009); *Estrategia Europea de Seguridad;* Consejo de la Unión Europea; Bruselas; p.15

de seguir trabajando en la concientización de las personas sobre las tecnologías de la información e intensificar la cooperación internacional.

Aun siendo un análisis reflexivo sobre lo que hace falta para la UE, la realidad es que su revisión a profundidad no llega a materializarse. Si bien, trajo consigo el análisis a temas nuevos, la estrategia se mantuvo y no se mencionaron mecanismos para solucionar aquellos problemas que se presentaron. En general, todo el documento no abordó algo en concreto ni práctico, solo mencionó algunas debilidades y los trabajos arduos que se han hecho. Igualmente, insta a todos a trabajar y cooperar con la UE para poder lograr los objetivos del mundo cambiante pero sin presentar medidas para adoptar contra las amenazas.

> El Informe tiene motivos para ser complaciente porque las políticas europeas de ampliación y de vecindad han producido resultados muy positivos en el ámbito de la prevención de conflictos, desde el Mediterráneo hasta el Cáucaso pasando por Oriente Medio, y en el normativo, apoyando todos los esfuerzos normativos multilaterales para prevenir y solucionar los problemas de seguridad que puedan afectar a la periferia europea. Sin embargo, para ser una Europa más eficaz y capaz dentro de un mundo en cambio no basta con acumular misiones sino que es necesario asegurar resultados.[108]

Tampoco hace una mención importante respecto a los escenarios internacionales en los que se encuentra. No habla de los países con quienes tiene conflicto o con quienes ha mejorado relaciones. Hace mención de China y la ampliación de sus relaciones, de Rusia solo menciona el conflicto en Georgia y cómo esto podría afectar, aún más, sus relaciones. No hace ninguna mención más importante y tampoco desarrolla relevante.

Las fallas que presentó el Informe pueden ser ocasionadas por todos los hechos que vivía la UE en esos momentos. La presidencia del Consejo de la Unión Europea estaba a cargo de Francia que dentro de su Libro Blanco sobre Seguridad Nacional y Defensa acababa de definir un proyecto para Europa en esta área pero el referéndum irlandés[109] respecto al Tratado de Lisboa había

[108] Arteaga, Felix; La Estrategia Europea de Seguridad, cinco años después*; Real Instituto El Cano Royal Institute*; Recuperado en: http://bit.ly/2nHUwPr

[109] El referéndum irlandés buscaba ratificar el Tratado de Lisboa que establecía "Una constitución para Europa". Debido a que el referéndum obtuvo una respuesta negativa se realizó un segundo referéndum que ahora si aprobaba la ratificación al Tratado. El referéndum se lleva a cabo debido a la modificación

complicado el establecimiento del proyecto francés. Además del enfrentamiento entre Rusa y Georgia, la crisis financiera del final del semestre de ese año[110], las complicadas relaciones militares y políticas con la Organización del Tratado del Atlántico Norte (OTAN)[111], las malas relaciones greco-turcas, la actualización de los acuerdos de Berlín Plus[112], las diferencia coyunturales en las operaciones en Afganistán en donde varios Estados europeos no estaban de acuerdo en participar en las operaciones militares.

Junto con todo esto, lo más evidente y uno de los mayores retos para la presidencia francesa era las desigualdades en el reparto del esfuerzo de seguridad y defensa entre los Estados miembros.

> No se han establecido mecanismos que permitan redistribuir equilibradamente el esfuerzo militar. Aunque en cifras globales los 27 miembros de la UE presupuestan el 20% del gasto mundial anual de defensa (207 billones de euros), su estudio revela que la mayoría de esos fondos se pierde en gastos de personal (unos 2 millones) en lugar de hacerlo en inversión y tecnología para facilitar la proyección de las fuerzas europeas (unos 60.000). También revela que sólo unos pocos de los 27 realizan un esfuerzo para sostener la capacidad militar de la UE, mientras que el resto son neutrales, carecen de capacidad militar o, simplemente, son consumidores de seguridad. En este contexto de contribuciones desiguales, escasas e ineficientes resulta muy difícil sacar adelante estrategias colectivas, por lo que de haber entrado en vigor el Tratado de Lisboa, la Presidencia francesa habría impulsado las cooperaciones reforzadas o las cooperaciones estructuradas permanentes para dar cuerpo a la autonomía estratégica europea.[113]

En general, los acuerdos se vieron malogrados por las diferentes visiones de los gobiernos de los Estados miembros sobre los acontecimientos más relevantes. El despliegue de la Organización del Tratado del Atlántico Norte

---

de algunos artículos en la Constitución de Irlanda en las que no se permitía que otras leyes estuviesen sobre la constitución, en especial las de la UE.

[110] La crisis financiera de 2008 se desata debido al colapso de la burbuja inmobiliaria de Estados Unidos. Las repercusiones comenzaron a inicios de 2008 en donde primero afectó al sistema financiero estadounidense y después al sistema internacional. Esta crisis produjo una profunda crisis de liquidez que trajo consigo los derrumbes bursátiles y la crisis económica a estala internacional.

[111] Tras la desintegración de la URSS, las relaciones entre la UE y la OTAN ya no tienen intereses compartidos. En su mayoría los choques se dan por los miembros de la UE que no están de acuerdo en algunas imposiciones de la OTAN o en operaciones militares como lo fue Afganistán.

[112] Los acuerdos Berlín Plus se adoptan en marzo de 2003 sientan bases de cooperación entre la OTAN y la UE en el ámbito de la gestión de crisis, esta permite a que la OTAN apoye las operaciones dirigidas por la UE en las que no participa la OTAN en conjunto.

[113] Arteaga, Félix; Op. Cit. Recuperado de: http://bit.ly/2nHUwPr

(OTAN) a Afganistán tampoco facilitó el concretar una Estrategia Europea de Seguridad más fuerte y lo que vendría en 2009 y 2010, en Afganistán, sería un elemento de choque entre las diferentes visiones de los miembros. Y aún el informe fue una buena manera de considerar las deficiencias de Europa, la realidad es que para ese momento era necesario un estudio a profundidad que pudiera transformar y modificar la Estrategia para solucionar de una buena forma todas las amenazas para las cuales la UE no parecía del todo preparada.

2.7 European Public-Private for Resilience (EP3R) (2009)- las PPPs

La relación entre lo público y lo privado para la Unión Europea ha representado un punto importante para el desarrollo de muchas de sus políticas en diferentes sectores. Esto trajo consigo la necesidad de crear alianzas que pudieran complacer a los intereses públicos como a los intereses privados. Este es un punto importante a tratar porque gracias a estos acuerdos se logra una mejor coordinación al momento de establecer políticas públicas en donde todos los sectores se vean beneficiados y puedan trabajar en conjunto.

La apertura a la participación del sector privado en diferentes áreas es un primer paso al trabajo en conjunto. El que los órganos comunitarios recurran a la experiencia del sector privado para mejorar la eficiencia de la construcción, la calidad de la gestión y explotación de las infraestructuras a partir del gasto fiscal ha sido uno de los primeros propósitos para la creación de esta asociación, además de que era necesaria la participación de lo privado para la apertura comercial en toda la UE.

Para lograrlo, la UE crea la Asociación Europea para la Resilencia Público-Privada (EP3R) o su nombre original, European Public-Private for Resilience. Esta asociación especial se encargaría de las alianzas en el sector de seguridad de redes de información y resiliencia en Europa. Las partes interesadas fueron las que pertenecen a las Telecomunicaciones y al Sector de la tecnología de información. Esta asociación se logra establecer en 2009 y comienza con discusiones respecto al compromiso de cada una de las partes en la seguridad, además de cubrir algunas lagunas sobre el crecimiento de las telecomunicaciones en los últimos años.

Los debates de esta asociación duraron cuatro años en donde se buscó evaluar, en un primer momento, el impacto que tiene esta asociación en las Infraestructuras Críticas. En el apartado 2.5 se hace mención a que varias de las IC no pertenecen únicamente a los gobiernos, algunas son de carácter privado o el sector privado ha invertido en las IC más importantes a nivel nacional. Es por ello que el trabajo conjunto en ambos sectores, es fundamental para el buen funcionamiento del Estado.

En esta primera parte del informe de EP3R se revela que el sector de las IC de la información está fragmentado debido a la competencia entre operadores de telecomunicaciones. También habla de la necesidad de crear una capacidad de recuperación (resiliencia) para cuando las IC fallen y establecer una preparación cooperativa entre lo público y privado a nivel nacional para mejorar la respuesta en cualquier falla que pueda tener cualquier IC y por cualquier tipo de causas. Además, se busca crear procedimientos transfronterizos que permitan una mejor conducción a las fallas que puedan tener las IC europeas.

De este primer encuentro, la Comisión Europea establece una primera iniciativa política llamada “Protección de Infraestructuras de Información Crítica (CIIP)”. De la misma forma, plantea cuatro objetivos a seguir dentro de la coordinación Público-Privado:

- Fomentar el intercambio de información y la recopilación de buenas prácticas políticas e industriales para fomentar el entendimiento común
- Discutir las propiedades, objetivos y medidas de las políticas públicas
- Establecer procedimientos básicos para la seguridad y resiliencia
- Identificar y promover la adopción de buenas prácticas en lo que se refiere a la seguridad y la resiliencia.

Durante las discusiones, se buscaba una reglamentación que pudiera permitir la realización de proyectos de las IC en conjunto con el sector privado, además de establecer una serie de actos comunitarios que facilitaran esta reglamentación. Se crearon, a partir de la iniciativa de Protección de CIIP, entre lo público y lo privado, una serie de directivas y libros verdes que establecían

ciertas normas en esta asociación, además de los procedimientos a seguir por parte del sector público al momento de firmar contratos con el sector privado.

Todas las directivas y libros verdes que salieron de estas reuniones eran meramente consultivas aunque no le resta importancia pues con ellos se logran crear procedimientos que después tendría importancia en las reformas legislativas comunitarias. En 2004, el mismo año de los primeros debates, se crean directivas de coordinación a los procedimientos de adjudicación de algunos contratos de Estado. La Comisión Europea también publica un "Libro Verde sobre la colaboración público-privada y el derecho comunitario en materia de contratación pública y concesiones". Con estos antecedentes se busca introducir una regulación común europea que permita la colaboración amigable entre el Estado y el sector privado.

En 2011, comienza la segunda parte en donde ENISA interviene publicando una Guía de buenas prácticas sobre modelos cooperativos. Fueron muchas reuniones entre los participantes que llevaron a abordar los problemas complejos de cooperación dentro de los diferentes posibles escenarios. De estas reuniones se estableció que se necesita alcanzar un nivel alto de madurez en el sector de las telecomunicaciones en 4 puntos principales:

- Implementar PPP (Programas Público-Privado) ágiles que se puedan adaptar a nuevas necesidades y temas
- Incentivar las iniciativas de la industria
- Definir reglas formales por parte de los gobiernos
- Publicar y publicitar resultados exitosos

A partir de ellos, se puede decir que:

> El gran número de experiencias de PPP en todo el mundo ha confirmado el valor de dicho enfoque también por su flexibilidad y adecuación para los desafíos emergentes actuales, incluida la mitigación de ataques cibernéticos, la protección de infraestructuras críticas y la seguridad y la capacidad de recuperación de la información y las comunicaciones. Este estudio propone investigar la brecha entre las características óptimas esperadas de una Alianza Público Privada para la Resiliencia y su implementación en el EP3R.[114]

[114] ENISA (2015), Conclusion for the European Public-Private Partnership (PPP) for Resilience scheme*; ENISA,* Recuperado de: https://goo.gl/fst3Qw

Los objetivos que buscaba alcanzar todo este análisis se resumen en comprender las alianzas público-privadas en el sector de las telecomunicaciones, comprender qué necesidades existen para poder mejorar la red y la seguridad de la información a nivel paneuropeo y hacer una prospectiva del impacto, de forma positiva, de esta cooperación de los procedimientos que se establezcan en estas reuniones.

Algunos de ellos fueron:

- El libro verde sobre la modernización de la política de contratación pública de la Unión Europea. Hacia un mercado europeo de la contratación pública más eficiente (2011): Se plantean introducir reformas sobre la contratación pública del 2004.
- Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la Contratación Pública y la derogación de las iniciativas 17 y 18 del 2004 (2011): siguiendo lo propuesto en el libro ver al respecto.
- Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adjudicación de contratos de concesión (2011): plantea que la UE necesita crear normas comunes sobre concesiones.
- Libro Verde sobre la Colaboración Público-Privado (2014): establece directivas sobre normas de adjudicación de contratos de concesión y contratación pública.

Todo esto permitió satisfacer el interés de que la colaboración con el sector privado permitiera el desarrollo de nueva infraestructura y la prestación de servicios públicos, debido a la limitada capacidad presupuestaria de los Estados. Esto evitaría el endeudamiento público para el financiamiento de las IC y permitiría un mejoramiento a los servicios. Aun así, esta colaboración no ha tenido el éxito que se pretende en todos los Estados miembros. Debido a que no se han puesto en la mesa los resultados de esta colaboración, no se ha examinado los fallos que ha tenido en algunos de estos países.

Un ejemplo clave es España y su sistema sanitario, debido a algunos desconocimientos de cómo funcionan los modelos de colaboración público privada. Los modelos que se han utilizado son las concesiones administrativas, las iniciativas de financiación privada, las adjudicaciones de atención sanitaria

de área de la población, las derivaciones sistemáticas del sector privado, entre otras. Ninguna se ha evaluado, dentro de la administración española, de forma transparente y han incrementado los costos en tratamientos médicos o en diagnósticos.

Es importante considerar tanto las cosas positivas como negativas de esta asociación. Aunque es bien sabido que estas iniciativas han logrado mejorar algunos sectores de la UE, tenemos que tener en cuenta los posibles problemas que también pueden enfrentarse. En la cuestión del ciberespacio, un ejemplo podría ser la asociación de lo público y privado en las cuestiones de ciberseguridad. Empresas privadas contratadas para mejorar la seguridad de un actor multilateral podría traer algunos problemas, en especial con la apertura comercial.

Los costos de la ciberseguridad podrían aumentar según la demanda tanto de los ciudadanos como de las instituciones nacionales o de la misma UE, además de que podrían existir monopolios, en inicio, respecto a la seguridad pues aunque la UE se excusa de un libre mercado, se le han dado favoritismo a diferentes empresas.

En junio de 2017, Kaspersky acusó a Microsoft de no permitir igualdad de condiciones de competencia para el resto de los fabricantes en la cuestión de seguridad. En la última versión de Windows 2010 se crean obstáculos para la competencia en las soluciones de seguridad y obliga al usuario a solo utilizar un software de seguridad creado por Microsoft. Se acepta la acusación de Kaspersky y se hacen multas a Microsoft. Tras largas investigaciones y pláticas, a finales de ese mismo mes Microsoft actualiza su software para que terceros puedan funcionar sin problemas, aunque fue solo *Kaspersky* que dio opiniones favorables al respecto y retiro la queja.[115]

Como se puede ver, las empresas privadas tienen un rol muy importante en las cuestiones que competen al Estado. Pese a ello, la asociación público-privado ha demostrado ser más favorable para el sector privado, en especial las empresas que tienen más influencia en la región. El caso de Microsoft contra Kaspesrky es una prueba de ello, demuestra las empresas que tienen más poder dentro del sector informático en la UE. Son las empresas grandes

[115] Iglesias Fraga, Alberto (2016), Kaspersky acusa a Microsoft de inhabilitar antivirus de terceros, *TIC beat*, recuperado de: https://goo.gl/iu2w9i

que mantienen una influencia dentro del Estado y este a su vez se beneficiado con su colaboración para el progreso europeo.

Y es tan necesario su colaboración que el Consejo Europeo pidió, en noviembre de 2017, a las empresas más importantes del sector informativo y comunicaciones el colaborar en la defensa de los Derechos Humanos dentro de Internet. Esta colaboración solo tuvo en cuenta a las empresas grandes y más influyentes del mercado europeo como son Apple, Microsoft, Kaspersky, Deutsche Telekom, Facebook, Google, Orange y Telefónica.

Si bien, la asociación público-privado ha traído algunos beneficios es necesaria la aplicación de procesos de transparencia realmente aplicables a toda la labor de las empresas privadas, en especial si se busca la conformación de una política de ciberseguridad fuerte. Y en este caso solo hablo de ciberseguridad pero cualquier aspecto con la Seguridad y Defensa necesita una buena coordinación de público y privado, para ello la clave de todo es la transparencia en los procesos en el que participen ambos sectores.

2.8 Estrategia de Ciberseguridad de la Unión Europea (2013)

Aunque anteriormente surgieron directivas y planes para la protección del ciberespacio como: Estrategia para una sociedad de la información segura (2006) o Un enfoque global para la protección de datos personales en la Unión Europea (2010), el objetivo era el mismo que se iba repitiendo anteriormente: la seguridad de datos personales, implementar mecanismos al respecto y la cooperación. El resultado era el mismo al final, un plan o estrategia que no contenía instrumentos suficientes o eficaces que cumplieran con los objetivos planteados y aunque si procuró la protección de datos de los usuarios, sigue sin imponer a nivel Unión una estrategia que enfrente a los retos y amenazas que se han tratado desde el año 2001.

Es el año 2013, un año importante para la Seguridad para la Unión Europea debido a los nuevos temas que se ponen a discusión en el Consejo Europeo y el establecimiento de la ciberseguridad como tema de prioridad. Es a inicios de este año en que se publica, por primera vez, una Estrategia de Ciberseguridad para la Unión Europea. Es un hecho que trasciende debido a que al fin se ven concretos todos los esfuerzos que realizó la UE desde inicios

de 2001 hasta el 2013, largos años en que el debate y el análisis debieron ser parte de la creación de esta Estrategia.

El nombre que recibe esta estrategia es “Un ciberespacio abierto, protegido y seguro” donde se plantean las visiones conjuntas sobre las cuestiones que la UE debe prevenir y resolver. El objetivo principal de la Estrategia es promover los valores europeos para estimular el crecimiento de una economía digital. Presenta las prioridades de la política de la UE con relación al ciberespacio. La cuestión es que esta estrategia de ciberseguridad fue de gran trascendencia porque plantea una amenaza en la cual se ha trabajado durante varios años pero de igual forma no establece mecanismos concretos para combatirla.

Como primer punto a esclarecer, se hablará de lo que propone esta nueva ciberestrategia. Se plantea que la iniciativa de esto es que los valores y derechos con los que se creó la UE sean aplicados al ciberespacio. Aplicar leyes, normas y valores que se tienen en el mundo físico al mundo virtual. Además de que busca que todos los actores que participan en la dinámica de la Unión Europea participen en esta migración al mundo virtual para lograr con mejor éxito el desarrollo de esta estrategia. Y obviamente, como punto fundamental para la UE, impulsar la cooperación internacional para conseguir un ciberespacio seguro, libre y abierto.

> Ha sido este ciberespacio abierto y libre el que ha promovido la integración política y social en todo el mundo; el que ha hecho caer fronteras entre países, comunidades y ciudadanos, potenciando la interacción y el intercambio de información e ideas de todo el planeta. […] Las tecnologías de la información y la comunicación se han convertido en la piedra angular de nuestro crecimiento económico y constituye un recurso crítico del que dependen todos los sectores económicos. Actualmente reposan en ellas los complejos sistemas que permiten funcionar a nuestras economías en sectores clave tales como las finanzas, la sanidad, la energía y los transportes. […] Las autoridades de terceros países pueden emplear abusivamente el ciberespacio para ejercer vigilancia y control sobre sus propios ciudadanos. La UE puede contrarrestar esta situación fomentando la libertad en línea y velando por el respeto de los derechos fundamentales en la red. […] Pues los Gobiernos del mundo ya han comenzado a desarrollar estrategias de ciberseguridad y a considerar el ciberespacio un asunto

> internacional cada vez más importante. Ha llegado el momento que la UE intensifique su intervención en este ámbito.[116]

El propósito de la UE para crear la estrategia de ciberseguridad no se aleja mucho de los primeros planteamientos al respecto: prevenir daños posibles que puede traer el ciberespacio para la economía moderna que quiere representar la UE. Para conseguirlo, se trazan algunos principios que van a presidir la política de ciberseguridad que podría plantearse a un nivel más internacional.

- Los valores esenciales de UE lo son tanto en el mundo físico como en el digital: Aplicar las leyes y normas físicas al ciberespacio.
- Protección de los derechos fundamentales, la libertad de expresión, los datos personales y la intimidad: Basar la seguridad en los derechos fundamentales y las libertades enunciados en la Carta de los Derechos Fundamentales de la Unión Europea.
- Acceso para todos: Crear acceso ilimitado a internet eliminando las desventajas para los ciudadanos europeos. También buscar facilitar la conexión a aquellos con alguna discapacidad física.
- Gobernanza multilateral democrática y eficaz: La UE respalda la importancia del modelo de gobernanza de internet.
- Garantizar la seguridad: una responsabilidad compartida, ofrecer una respuesta coordinada a cualquier amenaza para reforzar la ciberseguridad.

Como segundo punto, plantea medidas estratégicas que se llevaran a cabo para defender el entorno en línea para lograr una libertad y seguridad que beneficie a todos. Articula cinco prioridades para las estrategias que se planteen para resolver los problemas:

- Lograr la ciberresiliencia
- Concienciación
- Reducir drásticamente la ciberdelincuencia

[116] Comisión Europea (2013); *Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro;* Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad; Bruselas, pp. 2-3

- Desarrollar estrategias y capacidades de defensa vinculadas a la Política Común de Seguridad y Defensa (PCSD)
- Desarrollar recursos industriales y tecnológicos de ciberseguridad
- Establecer una política internacional coherente del ciberespacio para la Unión Europea y promover los valores esenciales de la UE

Se plantea, de igual forma, la coordinación con el sector privado. Esta parte especifica mucho su participación, de crear compromisos pues su apoyo contribuye a un mayor fomento de la ciberseguridad. “Es conveniente que el sector privado [sic] desarrolle a nivel técnico sus propias capacidades de ciberresiliencia y comparta mejores prácticas con otros sectores [sic]. Los instrumentos creados por ese sector [sic] para responder a los incidentes, determinar sus causas y efectuar investigaciones forenses también deberían beneficiar al sector público [sic].”[117]

De igual forma, incita a los sectores más importantes del Estado, como transporte, energía, banca, bolsas, facilitadores de internet, entre otros, a evaluar los posibles riesgos que enfrentan en el ciberespacio y que pueden ser resueltos en los procedimientos tomados por la ciberseguridad de la UE. Se le otorgará apoyo a aquellas IC clave de cada Estado y que puedan perjudicar gravemente al mismo.

Tras los problemas que acontecieron en Estonia en 2007, de esto se hablará más a detalle en el tercer capítulo, y otros ciberataques que se recibieron en el resto de la UE, se recrean ejercicios que puedan estimular la cooperación entre los Estados miembros y el sector privado. Estos se conocen como CiberEuropa, el primero fue en 2010 y una de las participaciones más importantes fue la de Estonia. Los ejercicios son simulaciones de ataques y a partir de ello se comprende con qué rapidez se obtiene una respuesta tanto del sector público como del sector privado.

Los ejercicios se repiten y también promueven la creación de ejercicios de simulación en cooperación con Estados Unidos (CiberAtlántico) para comprender cómo sería una respuesta a un ataque en cooperación con uno de los socios políticos y económicos más importantes para la UE. Debido al éxito de estos ejercicios, el plan es buscar recrearlos con socios internacionales o

[117] *Ibíd.,* p. 6

con la misma OTAN para comprender tanto las debilidades como las ventajas en las respuestas a los ciberataques.

Uno de los puntos más débiles de la Estrategia es la ciberdefensa. Solo se promueve que exista en colaboración con otros organismos como la OTAN y alienta a que se desarrollen capacidades de ciberdefensa. No habla mucho al respecto e inmediatamente comienza con la cuestión del Mercado Único Digital. Como se ha visto a lo largo de toda la investigación se ha mencionado este tema en repetidas ocasiones y aunque no parezca relacionado con la investigación, es fundamental tenerlo en mente porque este siempre ha sido el objetivo a cumplir de la UE.

El problema surge cuando a lo largo de la historia de la ciberseguridad de la Unión no se han plasmado instrumentos sólidos que puedan convertir al Mercado Único Digital en una alternativa viable y segura. Existen muchas lagunas y muchas contradicciones tanto en las directivas como en los planes de seguridad con respecto al ciberespacio, además de que no se ha constituido un marco legal que prevenga todas las situaciones a las que se podría enfrentar este Mercado Único Digital que sería a partir de la constitución de las 28 economías y que podría representar una amenaza bastante evidente.

La estrategia de ciberseguridad es necesaria, especialmente en un actor multilateral que pretende modernizarse desde el ciberespacio y crecer a partir de ello. El problema es que al ser multilateral trae muchas fragmentaciones y choques de intereses ya sea por parte de cada uno de los Estados miembros o por sectores como el público y privado. Para poder lograr el liderazgo global que pretende la Unión Europea es necesaria la armonización tanto de las legislaciones nacionales como a nivel UE, además de tener una relación más cooperativa del sector privado.

Todo esto es con la intención de que se permita la creación de una Estrategia concisa que realmente represente un reto para quienes pretenden desafiarla. Esta Estrategia de Ciberseguridad es una base para los verdaderos propósitos a futuro pero hasta no se resuelvan las cuestiones de intereses, las responsabilidades pertinentes y la creación de mecanismos concisos de ciberdefensa, no se puede hablar de un avance real y que responda a los intereses y pretensiones de este actor multilateral.

2.9 El camino a la Seguridad Global de la Red: Towards a Europan Global Strategy (2013)

La Estrategia Global Europea fue creada por 4 países Suecia, Polonia, Italia y España con la perspectiva de 2030. Esto sucede debido a que la Estrategia de Ciberseguridad Europea no tiene un enfoque a largo plazo pese a que el ciberespacio se innova contantemente. Con esto se planea un documento que si pueda ver a futuro las posibles amenazas que se desean enfrentar y a las que se ve vulnerable el ciberespacio europeo y no quede tan falto de una visión a futuro. O por lo menos eso aparentaba ser en la propuesta.

> El ciberespacio es cada vez más importante para la integración global de las sociedades, por lo que requiere de acceso libre y seguro. La Unión Europea debería trabajar para aumentar la seguridad en las redes y la información, proteger las infraestructuras críticas de ciberataques y promover la evaluación, la armonización y el avance de los marcos jurídicos, sobretodo en el desarrollo de de mecanismos de verificación y aplicación. [118] [119]

Esta propuesta presentaba un proyecto que integrara a toda la UE para enfrentar desafíos importantes que están en el panorama internacional. Se trata de un documento con cuatro apartados que trataban de crear una política exterior de la UE con las prioridades más importantes: una Estrategia global para promover los intereses de los ciudadanos, principios rectores la política exterior, las prioridades de la acción exterior y de visión a la acción.

La primera, Estrategia global para promover los intereses de los ciudadanos, buscará promover la acción exterior de la UE a partir de la paz y seguridad de los ciudadanos europeos y tener capacidad de actuación en la asistencia mutua; la prosperidad, se necesita tener un mercado interno sólido y un sistema económico internacional ligado al desarrollo tecnológico; la democracia, promover los derechos humanos, libertades fundamentales y el Estado de Derecho; y un orden mundial basado en normas, que el Derecho

[118] *Ibíd*., p. 7

[119] Original: *Cyberspace is increasingly important to societies' global integration, and requires free and secure access. The EU should work to increase network and information security, protect critical infrastructures from cyber-attacks and promote the assessment, harmonization and advancement of new legal frameworks, particularly through the development of verification and enforcement mechanisms*

Internacional sea una verdadera garantía para el cumplimiento de la paz y la seguridad tanto de la UE como del exterior.

Los principios rectores la acción exterior son principios que se enfocan en la unidad de la UE y sus miembros para convertirse en un actor relevante a nivel global. Busca que a partir de la interdependencia en su actuar pueda constituirse como principal actor internacional. Las prioridades de la acción exterior repite los principios en los que se constituye la Estrategia de Ciberseguridad pero ahora para ser aplicables a una acción más al exterior por parte de la Unión:

- La primera es l*a seguridad de nuestra Unión* que es buscar una estrategia en cinco líneas de acción: la seguridad y defensa, la lucha contra el terrorismo, la ciberseguridad, la seguridad energética y la comunicación estratégica.
- La segunda es *la resiliencia estatal y de la sociedad de nuestros vecinos orientales y meridionales* que es crear una capa de resistencia a las amenazas a partir de la colaboración con los países vecinos.
- La tercera *Órdenes regionales de cooperación* se enfoca en crear una Estrategia compleja que cumpla los intereses de cada una de las partes desde las relaciones con los países vecinos y su interés estratégico en el Ártico.
- La cuarta es sobre *La Gobernanza mundial para el siglo XXI* busca la transformación de los órganos de gobernanza mundial y que sean acordes a la realidad internacional.

Sobre la visión a la acción se plantean 3 parámetros sobre lo que sería la inversión colectiva. El primero consiste en la credibilidad de la Unión, no es solo a partir de lo simbólico, se necesita estar toda la unión inmiscuida en los asuntos más importantes de política exterior. Desde la investigación hasta la lucha contra el cambio climático, la IC, la movilidad, el comercio, entre otros. Saber que hay un compromiso serio respecto a la posición que se desea tomar como actor de importancia global.

El segundo es la capacidad de respuesta que simplemente significa estar preparados para los cambios que vienen. Ser eficaz en las cuestiones de

la Seguridad y Defensa, se trata de ser más rápido en respuesta frente a cualquier tipo de crisis. Además, ser flexible ante las políticas de desarrollo y ajustar las prioridades estratégicas. Y el tercero es la integración pues, al ser un actor multilateral, necesita estar integrado en los ámbitos de actuación de la política exterior y de seguridad. Basarse siempre en la cooperación, especialmente entre los Estados miembros para poder implementar estos principios.

El documento busca conformar una Estrategia que le otorgue un papel más activo a la UE en las cuestiones de la política exterior. Como Estados Unidos o Rusia han sido actores muy activos en la realidad internacional, la UE pretende posicionarse como una influencia aún más fuerte. Esta Estrategia por lo menos eso pretende. Pero la cuestión que compete a la investigación vuelve a ser parte de un plano poco tentativo, la ciberseguridad se conforma a lo que ha venido siendo desde 2001 y no busca convertirla en un tema más importante para esta Estrategia de Exterior.

La Estrategia pretende que la UE se convierta en un actor relevante pero no logra cubrir todos los aspectos, en esta primera entrega, que debería de cubrir. La ciberseguridad es una de ellas pero si analizamos todos los planes, directivas o libros verdes, esta Estrategia solo enmarca los temas más sobresalientes de cada uno, que ya se han tratado y busca continuarlos a futuro pero siguiendo el mismo patrón, no hay mecanismos fuertes y se olvida de temas claves como la ciberseguridad, se convierte en un retroceso importante porque cuando ya está planteado en la mesa, esta política pretende regresarlo al archivo para seguir siendo trabajado muy aparte de los temas primordiales para la UE.

Podría decirse que esto se debe a muchos factores, los principales son: las diferencias en la construcción de políticas de seguridad por parte de los Estados miembros, las diferentes visiones de los Estados miembros sobre lo que debería y no ser la Política Exterior de la UE y las relaciones tanto con Estados Unidos como con la OTAN. Con ello no se pretende olvidar las relaciones importantes con otros países, como lo es con Rusia pero siendo Estados Unidos uno de sus socios más importantes y la OTAN una de las razones que los une, se debe considerar a este actor para sus decisiones a futuro con respecto a temas de seguridad.

Dentro de la UE se soslaya mucho la idea de crear fuerzas militares europeas que realmente funcionen para la defensa de la UE. Polonia y los países Bálticos son los primeros en apoyar esta idea. Además de que se considera que con la OTAN es suficiente para las cuestiones de defensa, al igual que construir una defensa europea podría traer algunos desacuerdos con la alianza ya creada con la OTAN y Estados Unidos. Esto ocurre porque países tanto de Europa central como oriental dependen del armamento estadounidense, en especial con las complicadas relaciones con Rusia.

> Por ejemplo, el llamado Grupo de Visegrado, formado por Polonia, Hungría, República Checa y Eslovaquia, ha hecho hincapié en la preocupación de que una Política Común de Seguridad y Defensa más fuerte podría ir en contra de la OTAN. Estos países consideran que la UE no ofrece, ni de lejos, las garantías de la Alianza Atlántica y de EEUU. Además, y aparte de las cuestiones presupuestarias, existen importantes reticencias para ceder más competencias a la UE en detrimento de los parlamentos nacionales.[120]

Esto también choca con otra idea, el que muchos ciudadanos europeos consideran que solo el Estado-nación es el que puede responder mejor en las demandas de seguridad y que es justo este trabajo en conjunto de la UE que impide que se puedan crear buenos mecanismo para el desarrollo de una Política de Seguridad y Defensa fuerte. Esto conlleva a regresar a la idea de los nacionalismos y esperar que sea el Estado el que realmente otorgue una solución, que trabajar en conjunto. Todos estos elementos han alentado la creación de una política de defensa y seguridad común europea.

Y la cuestión de la ciberseguridad es aún más problemático porque hay países, dentro de la Unión, como Alemania o Francia que cuentan con una estrategia de ciberseguridad fuerte y desarrollada mientras otros países van desarrollando este tema conforme lo desarrolla el Consejo Europeo o la Comisión. Al final el tema de ciberseguridad quedará rezagado a promover la seguridad de datos personales y la cooperación internacional.

[120]Laborie Iglesias (2016), Mario; Hacia unas nuevas (e impredecibles) relaciones OTAN-UE; *Revista Española de Defensa*; (No. 23) p. 55

2.10 Estrategia Global de la Unión Europea (2016)

Así como se presentó, en 2003, una Estrategia de Seguridad, que planteaba la seguridad solo para Europa, se presenta esta nueva estrategia absorbiendo aquellos temas que han quedado resegados desde hace varios años. La Estrategia fue llamada *Visión Compartida, la acción común: una Europa más fuerte,* (Estrategia Global de la Unión Europea), que presentaba una nueva visión estratégica para la política exterior, de seguridad y defensa. El documento se divide en 4 partes importantes: (1) Una estrategia global para defender los intereses de nuestros ciudadanos; (2) Principios directores de nuestra Acción Exterior; (3) Prioridades de nuestra Acción Exterior; (4) Desde la visión a la acción[121].

La primera parte repite todo lo que se ha discutido, proteger a los ciudadanos, sus datos y todo bajo el régimen del Derecho de Estado. La protección debe ser a nivel nacional y nivel Unión. El segundo apartado hace un hincapié a los principios que se seguirán en la cuestión de política exterior: Unidad, Compromiso, Responsabilidad y Colaboración conjunta para defender intereses comunes[122]. Se busca que deje de existir esa diferencia de intereses entre lo nacional y la Unión Europea. De igual forma, se deben asumir todos los problemas del mundo como lo es la pobreza, conflictos y los derechos humanos.

Este es un tema muy importante para la UE debido a todos los desplazados que llegan a su territorio para buscar auxilio y los problemas que han surgido al respecto como la venta de personas, las violaciones a mujeres, o la venta de esclavos. “La Unión Europea como actor global debe colaborar con otros actores para que conjuntamente defender los intereses comunes a escala global”.[123]

El tercer apartado es sobre las prioridades en las acciones con el exterior, este mismo se divide en 5 categorías: (1) La Seguridad de nuestra Unión; (2) La Resiliencia de los Estados y las sociedades del Este y del Sur; (3)

[121] Izquierdo, José de Carlos (30 de septiembre de 2016), La nueva Estrategia de Seguridad Europea 2016, *Instituto Español de Estudios Estratégicos,* p. 14
[122] *Ibíd.,* p. 15
[123] *Ibíd.,* p. 16

Una Perspectiva Integrada en los conflictos y crisis; (4) Las organizaciones regionales de cooperación. Y, (5) la gobernanza mundial en el siglo XXI[124].

> Para garantizar la Seguridad de nuestra Unión, según el documento, se debe trabajar en cinco líneas de actuación: (1) Seguridad y defensa, (2) Lucha antiterrorista, (3) Ciberseguridad, (4) Seguridad Energética y (5) Comunicaciones estratégicas. Por ello se exhorta que la UE debe estar lista para proteger y defender sus intereses frente amenazas externas, para lo cual debe responder a las crisis externas cooperando con la OTAN y otros aliados, sin perjudicar a los Estados miembros que no estén en la OTAN[125].

En este punto, en especial, es cuando trata con actores no estatales y se busca solucionar los conflictos y crisis con prevención, seguridad y estabilidad y una política económica que favorezca la paz, tal vez refiriendo a ampliar en las cuestiones de seguridad. Se debe garantizar la soberanía de los Estados y existir integración territorial para la resolución de conflictos.

En la cuarta parte, se habla de la Gobernanza mundial del siglo XXI, ya se hace a la idea de seguridad en las redes y promover la ciberdiplomacia. Además de ampliar la Unión Europea, apoyar el desarme multilateral y cumplir con los tratados del control de armas. Se reconoce al terrorismo como una de las amenazas más importantes y el descubrimiento de otras amenazas que pueden ser por otros medios. Se busca apoyar 3 elementos primordiales para poder establecer una política de Seguridad y Defensa útil: "(1) La Acción Diplomática contemplada en el Tratado de Lisboa; (2) Una Política Común de Seguridad y Defensa más rápida y eficaz; Y (3) el Desarrollo de políticas más flexibles y alineadas con nuestras prioridades estratégicas [sic]"[126].

La Estrategia Global pretende que exista comunicación política que pueda complacer todos los intereses de los Estados miembros. Además, ya comienza un planteamiento de una visión más actual, las cuestiones del ciberespacio comienzan ya a ser evocadas para prevenir riesgos o amenazas que puedan atentar a toda la paz y seguridad deseada. Los viejos temas también están incluidos porque son cuestiones que no perderán importancia en varios años, el caso de Rusia es uno de los importantes a tratar y los

[124] *Ídem*
[125] Izquierdo, José de Carlos op. Cit. p. 17
[126] *Ibíd.,* p. 19

inmigrantes o desplazados también son una carga para la seguridad de la Unión Europea.

2.11 El futuro de Europa

Como se ha visto a lo largo de la investigación, la Unión Europea busca constituirse como un pionero en las cuestiones de ciberseguridad. Es por ello que el debate dentro de estos temas sigue siendo muy arduo y sin llegar a conclusiones concretas al respecto. Además, considerar que la naturaleza misma del ciberespacio no permite que se establezcan normas de regulación, como puede ocurrir en otros territorios, lo que impide que se logre un acuerdo y surjan, aún más, cuestionamientos al respecto. Por ello, ha planificado la creación una Agenda Digital que permita la innovación de la Unión y la ampliación del Mercado Único al ámbito digital

2.11.1 La Agenda Digital Europea

Los objetivos 2020 (Estrategia Europa 2020), es la Estrategia que tienen la UE para el crecimiento y el empleo de la Comunidad Europea. “Señala el crecimiento inteligente, sostenible e integrador como manera de superar las deficiencias estructurales de la economía europea, mejorar su competitividad y productividad y sustentar una economía social de mercado sostenible”.[127] Estos objetivos serán aplicados para un panorama global a partir de que se concreten los objetivos nacionales de cada miembro de la Unión.

La Agenda Digital para Europa es una de las primeras iniciativas para poder cumplir los objetivos planteados en la Estrategia Europa 2020. Los objetivos se conforman por los ámbitos del empleo, investigación y desarrollo, cambio climático y energía, educación; y pobreza y exclusión social. La Agenda busca una innovación y crecimiento económico para la UE que pueda ser aprovechado por los ciudadanos como por las empresas. Hay que recordar que todas las iniciativas de la UE siempre van dirigidas al crecimiento y mejoramiento del Mercado Europeo. En este caso, se dirigirá a la cuestión de Internet.

[127] Comisión Europea (2015), Estrategia Europa 2020. *Gobernanza Económica de la Unión Europea*. Recuperado de: https://goo.gl/gP9pgf

La Agenda Digital se agrupa en 7 pilares importantes:

1. Un mercado único digital
2. Interoperabilidad y normas
3. Confianza y seguridad
4. Acceso rápido y ultrarrápido a Internet
5. Investigación e innovación
6. Fomento a la alfabetización, la capacitación y la inclusión digital
7. Beneficios que hacen posible las TIC para la sociedad de la UE

La economía digital ha aumentado en todo el mundo. Pero la UE se ha caracterizado por no tener redes que satisfagan las necesidades de estas nuevas formas en que se mueve la economía.[128] Los costos diferentes en los países sobre el internet, la conectividad a diferentes velocidades han sido una brecha digital para el crecimiento del mercado digital en la UE. Se estima que para 2020, 16 millones de puestos laborales requerirán de conocimientos tecnológicos y existe una carencia importante en personas que realmente pueden manejar los avances de la tecnología.

> Los principales obstáculos para "estar conectados" son la falta de interés, la carencia de habilidades y de equipamiento TIC y los costes de la conexión a Internet. Sólo un 38% de usuarios de ordenadores tienen un nivel medio-alto de habilidades operativas TIC y un 30% lo tienen de habilidades relacionadas con Internet. Los países con mayores porcentajes de usuarios de ordenador tienden a tener un mayor número de personas con un nivel medio-alto de habilidades TIC.[129]

Estos obstáculos pueden tener efectos contrarios en la economía europea. Es por ello que se busca desarrollar cierto nivel de habilidades en las redes. Se buscará que no importe la edad, el género, el nivel educativo, la situación laboral o los ingresos familiares para que puedan ser desarrolladas estas habilidades. De igual manera, se pretende apoyar con personal

[128] Estonia, pese a ser uno de los países más desarrollados en seguridad y tecnología, las redes de navegación no soportan algunos sitios en internet estadounidenses debido a todos los elementos que la componen.

[129] Comisión Europea (2014), Comprender la políticas de la Unión Europea, *Agenda Digital para Europa*, Bruselas, p. 5

capacitado que pueda ser útil en cualquier aspecto de la vida para no dejar a nadie al margen de esta revolución digital.

Aún hay una gran brecha entre países. Se necesitan aumentar la participación de los mismos para poder potenciar este plan para la Unión Europea. El problema también radica en los intereses políticos y sociales, entre cada país miembro, que contrarían mucho a los objetivos económicos que pretende la UE para elevar su capacidad económica como digital. Pese ello, las propuestas de la Estrategia Europa 2020 siguen siendo claras.

2.11.2 El Mercado Único Digital

Una de las propuestas más codiciosas de la UE. Debido a algunos de los buenos resultados que ha presentado la economía en conjunto, como es el Mercado Único Común, se pretende buscar algo similar para la cuestión digital. La apertura comercial ha facilitado el movimiento del comercio en Europa pero no se ha actualizado para las empresas nuevas que surgen, las empresas digitales primordialmente. El objetivo del Mercado Único Digital es "garantizar la igualdad de acceso a los productos y servicios, establecer un medio adecuado para ecosistemas innovadores, dinámicos y seguros en Europa".[130] Esto mejorará las transacciones en línea y asegurará a los ciudadanos en líneas.

Unificar las 28 economías representará un reto importante. Entre ellos la ciberseguridad y la Infraestructura son elementos primordiales para conseguir que el Mercado Único Digital sea establecido con éxito. Además, se deben acordar diferentes cuestiones que permitan la liberación económica digital. Pero esta liberación se ha visto restringida por las diferentes economías debido a las cuestiones legales internas pues muchas no están de acuerdo con la apertura o chocan al momento de permitirla.

La propuesta del mercado parte de que se deben eliminar las tarifas de itinerancia. Esto significa que los dispositivos móviles podrán disfrutar del pago de las mismas tarifas y podrán navegar con sus datos móviles sin que existan restricciones por países. No habrá cargos por roaming o cargos de llamadas a

[130] Comisión Europea (2017), La UE y el Mercado Único Digital. *Comisión Europea.* Recuperado de: https://goo.gl/PzKC2o

larga distancia, será como si continuara en su país de origen con el mismo paquete de telefonía.

La cuestión de ciberseguridad es el segundo factor propuesto e importante del Mercado Único Digital. La idea es que se rijan a partir de la Estrategia de Ciberseguridad y la protección de ENISA. De la misma manera, se propondrán medidas adicionales en materia de ciberseguridad que puedan proteger todo el Mercado Único Digital. Aunque en este punto no se ha trabajado a fondo, solo busca continuar con lo propuesto por la Comisión sin hacer propuestas extra al respecto.

El fin del Mercado Único Digital es mantener a una Europa conectada y que se pueda acceder a un internet de gran calidad. Este punto es el que tiene un mayor apoyo pues se le destinarán 120 millones de euros para la financiación de los equipos que serán puestos en los sitios gratuitos. Estas normar pretenden ser aplicadas a los Estados miembros sin excepción a partir de 2018 y será necesario ir conociendo el éxito que tienen y qué nuevos retos plantean para la Unión Europea.

Es de esta forma que el debate sobre la seguridad de las redes, y su desarrollo en sí, ha sido constante sin que exista una concesión a nivel UE. La alternativa más fácil es la cooperación internacional. Es un constante en la UE respecto al tema pero ha sido esta cooperación la que ha permitido la creación de un Manual que podría representar para la UE una tentativa más formal a crear un marco legislativo en la cuestión del ciberespacio y de considerar una política exterior de ciberseguridad y defensa.

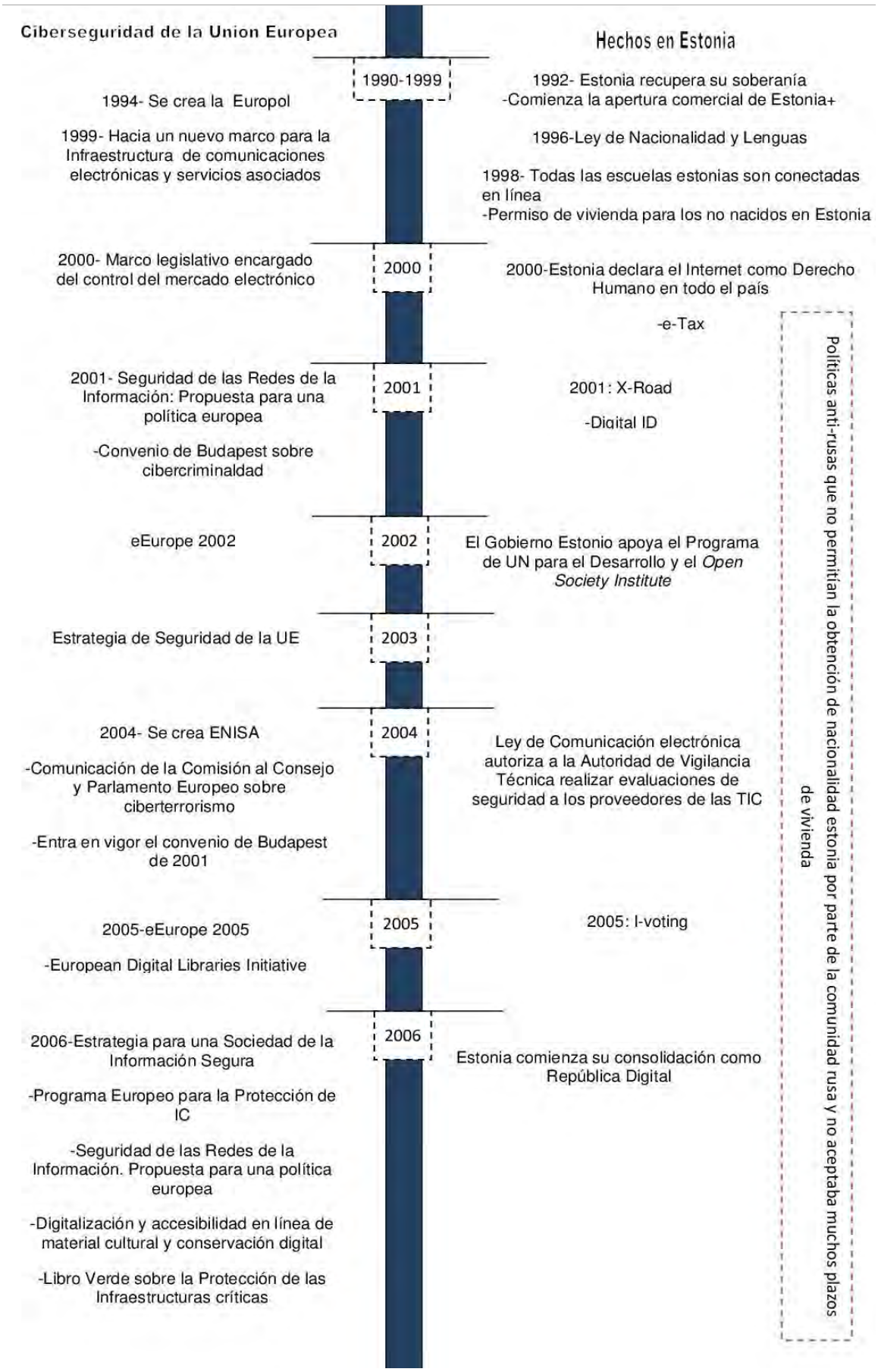
Este manual es importante porque sale justo de un conflicto ocurrido en el territorio europeo y se ha creado bajo la premisa constante de la UE, la cooperación internacional. Este manual se crea a partir de expertos en la materia de seguridad de diferentes países, además de la participación de la OTAN y Estados Unidos como colaboradores importantes al respecto. Este Manual es el Manual de Tallin que surge tras el conflicto cibernético entre Estonia, para ese entonces ya parte de la UE, y Rusia en 2007.

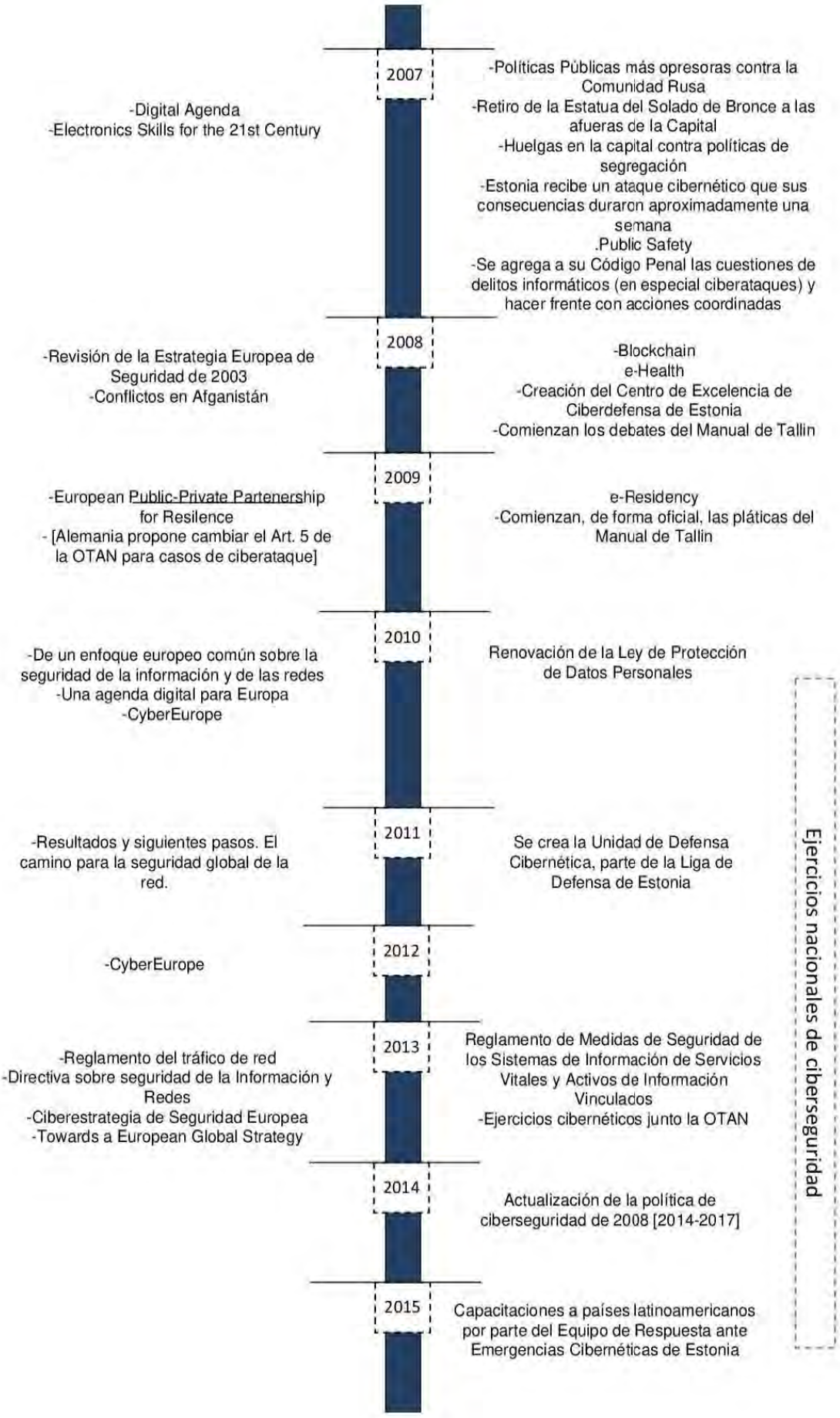
Antes que nada se debe aclarar que el Manual no es aún un instrumento legal aprobado, solo es un instrumento de investigación en el que diferentes países han aportado para la constitución de lo que podría ser, en un futuro, un marco legislativo internacional para el ciberespacio. Esto mismo lo hace un

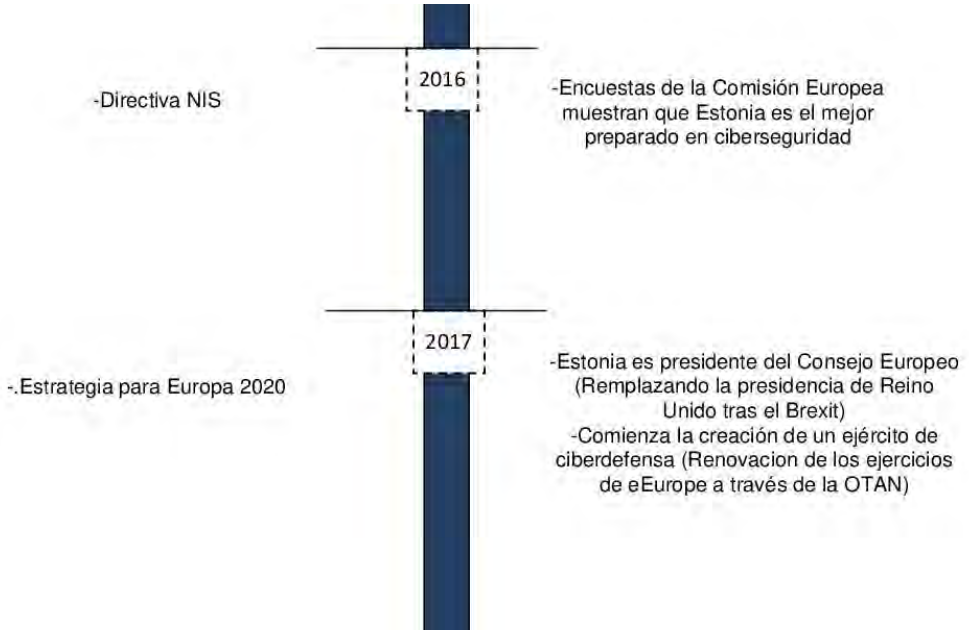
elemento importante no solo para la ciberseguridad de la UE sino para la ciberseguridad internacional porque sería el primer antecedente a la creación de un marco regulatorio que plasme las intenciones con el ciberespacio de todo el mundo. Y es importante para la UE porque podría quitar todos esos obstáculos que ha representado el crear una política tanto de seguridad y defensa como de ciberseguridad[131].

[131] Eliminaría la cuestión con la OTAN pues el organismo es parte de estas discusiones, además eliminaría el obstáculo de lo nacional pues sería a partir de lo internacional aplicarlo al margen nacional, aunque eso podría traer problemas a futuro pero ya sería modificarlo a partir de una base sólida y no solo se basaría en la protección de datos o cibercrimen sino en todas las amenazas que representa el ciberespacio, como la ciberguerra.

Línea del Tiempo sobre los acontecimientos en la Unión Europea y Estonia




2007
-Digital Agenda
-Electronics Skills for the 21st Century
-Políticas Públicas más opresoras contra la Comunidad Rusa
-Retiro de la Estatua del Solado de Bronce a las afueras de la Capital
-Huelgas en la capital contra políticas de segregación
-Estonia recibe un ataque cibernético que sus consecuencias duraron aproximadamente una semana
.Public Safety
-Se agrega a su Código Penal las cuestiones de delitos informáticos (en especial ciberataques) y hacer frente con acciones coordinadas
2008
-Revisión de la Estrategia Europea de Seguridad de 2003
-Conflictos en Afganistán
-Blockchain
e-Health
-Creación del Centro de Excelencia de Ciberdefensa de Estonia
-Comienzan los debates del Manual de Tallin
2009
-European Public-Private Partenership for Resilence
- [Alemania propone cambiar el Art. 5 de la OTAN para casos de ciberataque]
e-Residency
-Comienzan, de forma oficial, las pláticas del Manual de Tallin
2010
-De un enfoque europeo común sobre la seguridad de la información y de las redes
-Una agenda digital para Europa
-CyberEurope
Renovación de la Ley de Protección de Datos Personales
2011
-Resultados y siguientes pasos. El camino para la seguridad global de la red.
Se crea la Unidad de Defensa Cibernética, parte de la Liga de Defensa de Estonia
2012
-CyberEurope
2013
-Reglamento del tráfico de red
-Directiva sobre seguridad de la Información y Redes
-Ciberestrategia de Seguridad Europea
-Towards a European Global Strategy
Reglamento de Medidas de Seguridad de los Sistemas de Información de Servicios Vitales y Activos de Información Vinculados
-Ejercicios cibernéticos junto la OTAN
2014
Actualización de la política de ciberseguridad de 2008 [2014-2017]
2015
Capacitaciones a países latinoamericanos por parte del Equipo de Respuesta ante Emergencias Cibernéticas de Estonia
Ejercicios nacionales de ciberseguridad



Esta línea del tiempo está dividida entre la historia de Estonia tras su independencia de la URSS, los eventos en 2007 y las acciones tomadas después del desastre. La otra parte es sobre la historia de las políticas tomadas por la Unión Europea respecto a las cuestiones de telecomunicaciones y el ciberespacio.

Capítulo 3

Manual de Tallin y la configuración de una política de seguridad y defensa en la Unión Europea

> *Debido a las relaciones de identidad que se desarrollan dentro de un sistema, es posible crear un tipo de seguridad colectiva, capaz de preservar los intereses de los actores regionales inmersos en un sistema de cooperación interregional. El Estado no es el único actor en términos de seguridad y que los actores no estatales pueden generar cierta inestabilidad y, por lo tanto, conflictos. Las nuevas fuentes de amenaza suelen proceder de las condiciones de la vida cotidiana, antes que de la eventualidad de una guerra. Por ende, la protección de un Estado deriva no sólo de su unidad política, sino también del acceso de los individuos a poseer una adecuada calidad de vida*
>
> *Wojciech Kotescki*

El Manual de Tallin se ha convertido en un primer antecedente para lo que podría llegar a ser una legislación internacional sobre la regulación en la ciberguerra. El Manual explora varios aspectos, a partir de tratados de la guerra física, que pueden ser aplicables en el ciberespacio. Para poder comprenderlo en su totalidad, es necesario abordar el conflicto entre Estonia y Rusia sobre cuestiones étnicas e históricas que desencadenaron los sucesos del 27 de abril del 2007. Este suceso, de cierta manera, fue útil para la apertura del debate sobre la legislación del ciberespacio.

Se deben entender los efectos que este conflicto causó tanto a la seguridad estonia y la rusa como al debate internacional que vino años más adelante y que impulsarían tanto el Manual de Tallin como un Centro de Excelencia de la OTAN para la ciberseguridad, además de Directivas, dentro del Consejo Europeo, que impulsan la protección de las Infraestructuras Críticas (debido a que fueron las primeras afectadas) y la propuesta de actualizar el marco normativo propuesto por la UE para la protección de internet.

Aunque este conflicto pudo desencadenarse por cuestiones étnicas arrastradas del pasado soviético, también podría deberse a otras cuestiones no abordadas. Por ejemplo, la necesidad de la Unión Europea por consolidar una

política de ciberseguridad fuerte y que no se ha logrado crear debido a las diferentes posturas, o por una prueba de Rusia hacia Europa con respecto a canalizar la fuerza de los programas de ciberseguridad que se han buscado establecer a lo largo de la historia de la Unión Europea. Como fuese, es a partir de los incidentes de Estonia que la concepción del ciberespacio cambia para la comunidad europea.

3.1 Los incidentes en Estonia

Uno de los problemas que se encontró el gobierno soviético para poder unificar todo el territorio fue el de identidad, y fue un problema que tuvo bastante importancia a lo largo de lo que duró la Unión Soviética. Además de que en mucha formas se favoreció a Rusia, dentro de las repúblicas de la Unión. Es así como "la rusificación es ensayada en las repúblicas como la herencia de los condicionantes estratégicos del imperio zarista"[132]. Se buscó implementar diferentes políticas que permitieran la colonización de todo el país y se lograse una cohesión social sólida.

> Para Lenin el nacionalismo tanto ruso como el de las demás naciones del imperio constituía un obstáculo importante para el triunfo de la ideología marxista, que debía superar la estatificación étnica y económica al igual que otras supuestas consecuencias del capitalismo. Para llevar esto a cabo, Lenin ideó un sistema que aunaba el respeto a la autodeterminación, la igualación de los diferentes pueblos y la autonomía territorial. […] La igualación suponía en realidad la equiparación con la nación rusa, lo que exigía dotar al menos a los pueblos más relevantes del imperio de atributos similares, entre otros, de una base territorial[133].

Pero el problema surge cuando Lenin deja esta responsabilidad al partido comunista como representación del aparato central. "Este hecho no sólo suponía un límite evidente a esa autonomía, además es el origen de un intenso proceso de desinstitucionalización", o sea, la desaparición del Estado en donde el partido comunista sería su remplazo pero continuando con un poder céntrico. Continuando con la política propuesta por Lenin, Stalin pretendió seguir el esquema a partir de 3 problemas nacionales importantes: "el

[132]Pérez González, Ángel (2001), "Minorías rusas en la antigua URSS", *Afers Internacionals*, No. 52 p. 51
[133]Ibíd., p. 29.

nacionalismo ruso, los nacionalismos locales y la desigualdad nacional heredada del imperio zarista; considerando este último como la causa de los dos primeros. Su política tendió a buscar tal equiparación a través de una política de *indigenización*[134] formal de las nuevas repúblicas"[135].

Tabla 8. Cambios en la población de Rusia en el periodo 1917-1991

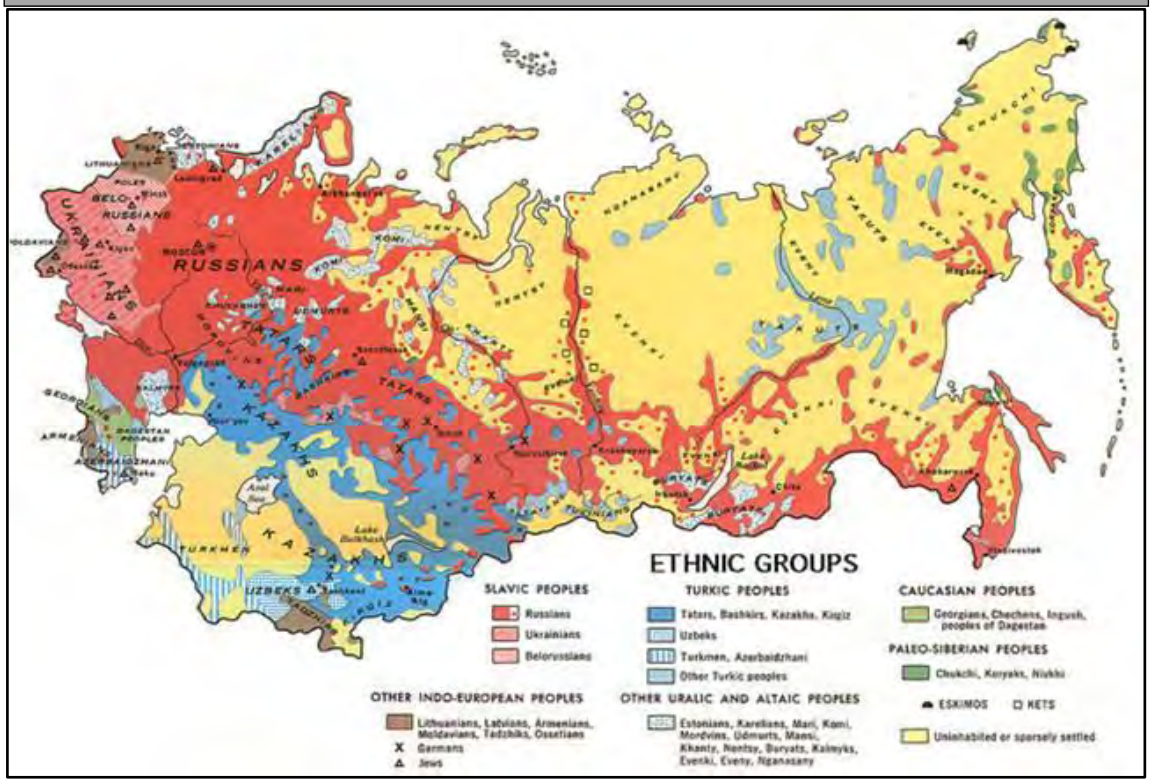
Periodo/años	Población al final del periodo/año, miles de personas	Crecimiento (descenso) de la población, miles de personas		
		Total	Crecimiento natural	Crecimiento migratorio*
1917-1926	93 600	-	-	-2 500
1927-1940	111 100	17 400	16 800	600
1941-1945	101 400	-13 453	-9 953	-3 500
1946-1950	101 400	5 398	6 505	-1 107
1941-1950		-8 050	-3 448	-4 607**
1951-1955	112 266	9 321	9 991	-670
1956-1960	120 766	8 500	9 283	-783
1961-1965	127 189	6 423	6 944	-521
1966-1970	130 704	3 515	4 107	-592
1971-1975	134 690	3 986	4 180	-195
1951-1975		31 745	34 505	-2 761
1976-1980	139 165	4 338	3 730	607
1981-1985	144 080	4 807	3 939	869
1986-1991	148 704	4 869	3 759	1 110
1976-1991		14 014	11 428	2 586
1917-1991		37 704	42 485	-6 882***

* Teniendo en cuenta el saldo migratorio con todos países. La parte correspondiente a los países de fuera de la ex Unión Soviética fue poco significativa en los años 1927-1940 y 1951-1987, destacando el periodo de 1917-1925, cuando más de 2.5 millones personas emigraron hacia Europa Occidental, Estados Unidos y otros países.
** De ellos, 700 mil personas emigraron fuera de la Unión Soviética.
*** De ellos, casi 3.6 millones de personas emigraron fuera de la Unión Soviética.
Fuente: elaboración propia a partir de los datos del Anuario Estadístico *Nacelenie SSSR v 1973*, anuario estadístico *Nacelenie Rossii za 100 let* y Andreev *et al.* (1998).

Fuente: Margarita Rohr Trushchelevea (2014), La evolución de demográfica y la importancia de flujos migratorios en Rusia: un recorrido histórico, *Revista de la Universidad de Valencia, Vol. 21, (*No. 86), p. 54

[134]O también Korenización (korenizatsia-коренизация) que significa nativización: Con el fin de terminar con el atraso económico y cultural se envían a rusos a poblar en las diferentes repúblicas de la URSS tratando de crear una cohesión social.
[135]Pérez González, Ángel (2001), "Minorías rusas en la antigua URSS", *Afers Internacionals*, (No. 52) p. 51
[135]*Ibíd.,* p. 29.

Mapa 7. Mapa de los Grupos Étnicos tras la desintegración de la URSS



Fuente: Fundación CIDOB, Los Conflictos de la Federación Rusa, *CIDOB*, (No. 26), p. 503

No obstante, su postura cambió debido a que su política fracasó y los nacionalismos locales comenzaron a ser un síntoma de inestabilidad en la URSS. Y aunque se permitirían las entidades territoriales de cada república, la realidad es que la política que se propuso favorecería una política de *rusificación*[136] que al final de la Segunda Guerra Mundial produjo la deportación de comunidades enteras de las diferentes repúblicas, muchas a Siberia. Esta sería una de las causas de la desestabilización interna de la URSS, además del alejamiento de relaciones con las repúblicas soviéticas.

Se crea la política del *"homo sovieticus*" que pretendía crear una identidad soviética en toda la URSS. "La ideología contribuyó de manera determinante a moldear tanto las mentalidades nacionales como la percepción del concepto mismo de nación"[137]. Aun así, el favoritismo siempre fue hacia los

[136]Implementación del ruso como lengua oficial.
[137]Pérez González, Ángel (2001), Minorías rusas en la antigua URSS, *Afers Internacionals*, (No. 52), p. 51

rusos y muy excluyente al resto de los territorios que también formaban parte de la URSS. Y es este nacionalismo excluyente el que genera, en los nuevos estados, "una pretendida homogeneidad que no ha existido en ningún sitio"[138]. En los estados bálticos se ha exaltado con mayor preponderancia el deseo de crear esta homogeneidad para olvidar la dictadura soviética que tanto los ha reprimido.

Debido al tamaño del territorio y la cantidad de población, esta exclusión de minorías fue más marcada en los países bálticos que los de Asia Central, como en "Kazajstán dónde los rusos representaban el 37 % de la población, [por ello] su integración fue modélica, pero en el Báltico la situación fue muy distinta".[139] Las políticas para la nacionalización fueron demasiado duras con los ciudadanos rusos. Y aunque en "Lituania se decidió que todos sus residentes pasaran a ser ciudadanos de pleno derecho del nuevo Estado, sin importar la etnia de origen [no significó lo mismo] para Estonia y Letonia donde los rusos superaban el 30%"[140] lo que representa una cantidad bastante grande y significaría tanto fuerza de trabajo para Moscú como las probabilidades de una nueva y posible reconquista del territorio por parte de Rusia.

Por ello, ambos países establecieron que sólo tendrían estatus de ciudadano estonio o letón "aquellos que tuvieran esa nacionalidad en junio de 1940 y sus descendientes. En lo que respecta a los llegados con posterioridad, podrían adquirir la ciudadanía tras un proceso de naturalización, que implicaba superar unas duras pruebas de conocimiento de las lenguas locales"[141]. Debido a estas políticas estrictas, muchos rusos no lograron la ciudadanía, algunos porque no querían perder la oportunidad de viajar a Rusia sin visado, otros porque eran personas mayores o personas enfermas que no eran capaces de superar las pruebas impuestas.

---

[137]Ibíd., p. 29.
[138]Ibíd. p. 32.
[139]Ídem
[140]Fundación CIDOB, "Los Conflictos de la Federación Rusa", *CIDOB*, No. 26, p. 504
[141]Ibíd. p. 505.

Tabla 9. Las Minorías rusas fuera de la Federación

LAS MINORÍAS RUSAS FUERA DE LA FEDERACIÓN ("EXTRANJERO CERCANO")

Población rusa en las antiguas repúblicas soviéticas (censo de 1989)

Estado	Total rusos (en miles)	% total población	% rusos *
ESTONIA	475.000	30,3	14
LETONIA	906.000	33,9	21
LITUANIA	344.000	9,4	33
BIELARÚS	1.342.000	13,2	25
MOLDOVA	562.000	12,9	11
UCRANIA	11.355.000	22,1	33
ARMENIA	52.000	1,6	32
GEORGIA	341.000	6,3	23
AZERBAIDZHÁN	392.000	7,6	14
KAZAJSTÁN	6.227.000	37,8	1
KIRGUIZISTÁN	917.000	21,5	1
TADZHIKISTÁN	388.000	7,6	3
TURKMENISTÁN	344.000	9,5	3
UZBEKISTÁN	1.653.000	8,3	5
TOTAL			**25.298.000**

*conocedores de la lengua del lugar de residencia

Fuente: Fundación CIDOB, Los Conflictos de la Federación Rusa, *CIDOB*, (No. 26), p. 503

Por mencionar un ejemplo, "la constitución estonia establecía que sólo los ciudadanos podrían ocupar cargos públicos, incluso a nivel local. Como consecuencia en la ciudad de *Narva*, donde el 95 % de la población eran rusos, nadie podía ser candidato en las elecciones locales, lo que obligó a relajar la legislación para estos casos extremos"[142]. Tampoco se puede decir que los estonios fueron los únicos *culpables de su desgracia*, la realidad es que estas

[142] *Ídem.*

medidas son la respuesta a las represiones vividas en el dominio soviético, los exilios a Siberia y todo el desajuste social que ocurrió en esa época.

La relación entre las Repúblicas Bálticas con Rusia siempre ha sido de tensión debido a la imposición del sistema socialista y todas las violaciones que existieron al momento en que se integraron, de forma forzada, a la URSS. Es por ello, que ahora las mismas acciones y actitudes se repiten para las minorías rusas. Y por más que las negociaciones con Rusia para que sus ciudadanos sean mejor tratados han ayudado un poco, es realmente difícil establecer una relación que beneficie a los rusos y esto produce, aún más, tensiones entre los países bálticos, en especial en Estonia.

La dependencia que tenía Estonia con Rusia era grande, aún ahora algunas cuestiones con el gas natural siguen obligando a Estonia tener relaciones políticas con Rusia aunque no lo desee. Hay que agregar también los descontentos de Rusia por la integración de los países bálticos a la Unión Europea y la OTAN. Aunque para estos países fue una estrategia crucial para alejarse de la influencia rusa y tener asegurada la protección de otras instituciones, era evidente que acrecentaría los problemas que ya se tienen con Rusia.

> Defendieron la tesis de que, una vez incorporadas en la UE y en la OTAN, ambos organismos obtendrían una ventaja competitiva debido a que sus puertos constituirían un enclave único para el desarrollo de las relaciones económicas, políticas y de seguridad entre Europa occidental y la nueva Europa del este, matizando la idea de que Rusia seguía representando una amenaza para su seguridad. {Aunque} la visión histórica rusa respecto a las tres repúblicas bálticas es que “fueron” y “son” parte del Imperio Ruso. La integración de los países bálticos en la UE y en la OTAN era percIbida por Moscú como una continuación de la guerra fría y un gran riesgo para su propia seguridad e integridad territorial.[143]

Teniendo presente la unión de los países bálticos a la UE y la OTAN, Rusia usaría cualquier pretexto para poder demostrar su fuerza frente a los intentos de alejarse más de su influencia. En específico, Estonia, debido a que su relación con Rusia es un poco más compleja que con Lituania y Letonia.

[143] Rodríguez Suárez, Pedro Manuel (Marzo 2015), Los países bálticos frente a Europa y Rusia, *Revista de la Facultad de Derecho y Ciencias Sociales*, (No. 37), México, p.p. 9-10

Estonia y Rusia han tenido choques más fuertes y esto ha acrecentado el odio de los estonios contra la comunidad rusa.

Se debe de entender que el suceso ocurrido en 2007 solo fue parte de los tantos conflictos que han tenido ambos países a lo largo de su historia respecto a las relaciones diplomáticas. Antes de ir en concreto al asunto, se debe entender cómo se fue desarrollando la economía de Estonia, tras la derrota del socialismo, para entender lo efectivo del ataque cibernético que se presentó y las razones por las que pudo ocurrir en esta nación.

3.1.1 e-Estonia: La estabilidad del Sistema Informático Estonio

Después de la independencia de Estonia, tras un largo período de gobierno soviético, comienza el largo camino al desarrollo tecnológico como se conoce hoy en día. Hay que recordar que bajo el gobierno soviético, Estonia no tuvo grandes oportunidades para desarrollar su tecnología pues "menos de la mitad de su población tenía una línea telefónica y el único medio de comunicación con los que están fuera del país y era controlado por Finlandia".[144]

Para 1992, cuando el primer ministro de Estonia, Martlaar, ocupó su cargo, buscó una forma de renovar la economía del pequeño país báltico. En menos de dos años, su gobierno tuvo grandes cambios en la economía de Estonia; como el adentrarse "al libre comercio, la moneda fuerte y la privatización. Además, se renovó la infraestructura soviética y tras negar el ofrecimiento de Finlandia de actualizar las conexiones telefónicas y digitales, Estonia construyó su propio sistema digital. De esta manera se crea un proyecto nacional para equipar las aulas con ordenadores y para 1998 todas las escuelas estaban en línea"[145].

Durante el 2000, "el gobierno declaró el acceso a Internet como un derecho humano y el Wi-Fi se convirtió en un espacio común siendo el primer paso para crear al *gobierno electrónico*. Con este nuevo *e-government* creó una nueva clase de inversores de Estonia, que hizo decenas de millones de

[144] A.A.K (3 julio de 2013), How did Estonia become a leader in technology?, *Way Back Machine,* Recuperado de: https://goo.gl/24rdzq
[145] *Ídem.*

euros de sus participaciones"[146].Lo que produjo la creación del *Tehnopo*l, que se convierte en el centro de negocios más importante de Tallin, alberga más de 150 empresas de tecnología. "Según el Banco Mundial, más de 14.000 nuevas empresas registradas en Estonia en 2011, 40% más que durante el mismo periodo de 2008. Las industrias de alta tecnología representan en la actualidad alrededor del [20%] del PIB"[147]. Es el Silicon Valley Europeo y es el referente tecnológico para la Unión Europea.

Sin embargo, es esta incursión al *e-government* lo que provoca que Estonia se viera vulnerable ante aquel que pudiera acceder y debilitar el sistema informático. "El aumento de la comunicación, el trabajo de la red y la dependencia a la infraestructura digital […] crea nuevas vulnerabilidades a los Estado-Nación"[148]. No es difícil, para un gobierno lograr atacar a otro con el que ha tenido problemas tanto de fronteras como de cooperación y el cual depende en un 97% de la tecnología para funcionar.

El *e-govermment* se logró implementar a partir de diferentes aspectos para digitalizar todo el país. En un primer momento aparece *e-Governance*, en 1997, que es una estrategia elegida por Estonia para impulsar las competitividades del Estado e incrementar el bienestar de las personas, mientras se implementa sin problemas la gobernanza. Los ciudadanos pueden elegir *e-soluciones* en donde el 99% de los servicios públicos son viables para los servicios.

Entre el año 2000 y 2001, existe una gran necesidad tanto de conectar a toda Estonia como el acelerar las operaciones con empresas para facilitar las formas de negocio. Se crean dos mecanismos importantes en la economía digital estonia, *e-Tax* y *x-Road. E*l e-Tax consiste en buscar soluciones fáciles que ayuden a configurar y administrar un negocio en Estonia. Esto promueve a agilizar los pagos de de impuestos tanto para empresas como para personas físicas. Este mecanismo facilitó tanto el pago de impuestos de cada año, en el país, que promueve la creación del X-Road. Se busca modernizar las funciones del gobierno, los trámites y facilitar los servicios para los ciudadanos. Con el *X*-

[146] Di Pace, Damián (2016); El Milagro de Estonia, la improbable meca tecnológica de Europa, *Infobae*, Recuperado de: http://goo.gl/a6xOrt

[147] *Idem*

[148] Herzog, Stephen (2011), Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Respons, *Journal of Strategic Security, (*No. 2), p. 51.

Road, se crean bases de datos para los servicios electrónicos de cada sector público.

Con ambos mecanismos, Estonia ya se catalogaba como un país avanzado, pese a las penumbras de su pasado. Aún así, el trabajo por digitalizar Estonia no se quedó en las bases de datos. Obligado por las exigencias de la Unión Europea de modernizarse para ingresar como miembro, continúa creando mecanismos que lo cataloguen como un país moderno y no con el recuerdo de que fue una ex-república soviética.

En el mismo año que se crea X-Road, también se busca que el acceso a la información de cada ciudadano sea fácil por parte del gobierno y para los servicios públicos, es así como se crea el *Digital ID* que consiste en una tarjeta con toda la información de las personas: datos personales, datos médicos, datos laborales y de seguros médicos o de vida. Además de que funciona para facilitar las operaciones bancarias, firmas de documentos o para obtener una receta médica.

Esta digitalización no busca quedarse solo en guardar los datos de las personas, sino realmente mover el país a través del mundo digital. Para 2005, Estonia se convierte en el primer país en el mundo en hacer su votación de elección nacional por internet. Pese a lo que podría presentarse como un problema de corrupción, las votaciones en Estonia fueron seguras, sin contratiempos y totalmente limpias debido a que cada ciudadano cuenta con su *Digital ID*. Esto es conocido como *i-Voting*, donde se permite que los ciudadanos voten a su conveniencia en sus casas o algún aparato electrónico que se lo permita. Este mecanismo ha facilitado el voto a quienes se encuentran en el extranjero o residen en otro país pero siguen siendo ciudadanos estonios.

Ha sido necesario facilitar todos los servicios públicos posible, para 2007 se promueve el mejoramiento a los servicios de seguridad pública. Se crea el *Public safety* que es fortalecer el orden público a través de herramientas informáticas. Es así como la policía, rescatistas o centros de emergencia han reducido la mitad de número de muertos por accidentes automovilísticos en los últimos 20 años. “Los servicios de seguridad pueden rastrear víctimas de un accidente de forma más sencilla, el 93% de las llamadas de emergencia son respondidas en 10 segundos y debido a que cada automóvil en estonia cuenta

con una computadora abordo que recupera los datos relevantes de algún accidente, ha mejorado la eficacia de la policía al momento de resolver los casos de accidentes de tránsito"[149].

Estonia funcionaba totalmente sin problemas, representaba el proyecto que la Unión Europea ha buscado a través de los años pero a escala de un país y funcionaba eficazmente. Pero de la misma forma en que funcionaba según lo proyectado, también tenía debilidades en algunas cuestiones. Estonia solo estableció las precauciones en el ciberespacio que la UE había establecido sin preocuparse de otras cuestiones que se venían trabajando en otras partes del mundo, como en Estados Unidos, respecto a las Infraestructuras Críticas o la intromisión a las funciones de gobierno a partir de virus informáticos como se había visto con el virus ILOVEYOU.

Es así que, con tal fragilidad en su ciberseguridad, el virus *DDOS*, que se introdujo en las computadoras de Estonia durante el enfrentamiento con Rusia a nivel cibernético, logró desequilibrar Estonia[150]. Además, demostró las debilidades tanto del proyecto estonio para digitalizar su país como el proyecto que venía preparando la Unión Europea sobre la protección de las infraestructuras críticas y la prevención a los ataques terroristas. Si para un país fue sencillo introducirse de tal manera, un intento terrorista sería aún más sencillo a gran escala.

De esta experiencia Estonia si buscó un camino más efectivo para la protección de su ciberseguridad que el que trabajaba la UE. En 2008, se crea el *Blockchain* a partir de las experiencias de los ciberoperaciones. Esta tecnología busca mejorar la seguridad en los ámbitos de salud, sistemas de códigos judiciales, legislativos, de seguridad y comerciales, la medicina personal, la seguridad cibernética y las embajadas de datos[151]. El *Blockchain* simplemente consiste en eliminar la centralización de datos.

> El blockchain es un método para registrar datos, una especie de archivo de Excel. Pero está compartido: existen copias en la Red y en los ordenadores de cada participante en la creación y modificación de ese archivo, al que no puede acceder cualquier persona sin permiso y en el que no se puede borrar información,

[149] Estonia Goverment (2001-2017). e-estonia. *Tallin, Estonia.* Recuperado de: https://e-estonia.com/#
[150] El tema se abordará complete en el siguiente apartado
[151] Se habla de estas en el apartado 3.4.1 de esta capítulo

> solo añadir nuevos registros. Esto permite que la colectividad se encargue de proteger los datos que contiene, alertando de posibles faltas de concordancia derivadas de cada actualización. Gracias a ello, se protege la integridad del documento[152].

Y siendo Estonia el pionero en esta tecnología, ha promovido su uso en la Unión Europea, la OTAN (en su Cooperative Cyber Defence Center of Excellence) y hasta en el Departamento de Defensa de Estados Unidos. Para este mismo año, se promueve e-Health que busca digitalizar todas las soluciones de salud para los ciudadanos. Este es el primer servicio que comienza a usar la blockchain para garantizar la integridad de los registros médicos digitales y los accesos a estos. La e-Health busca promover la salud en sus ciudadanos y agilizar los trámites médicos.

Tras la digitalización de los propios ciudadanos y con los propósitos de la propia UE, Estonia busca no solo dar estos beneficios a sus ciudadanos sino a cualquier persona en el mundo que quiera recibirlos, para esto crea una primera etapa que puede facilitar la apertura comercial: la *e-Residency.* Esta es una identidad digital trasnacional que puede proporcionar a cualquier persona que busque emprender en Estonia. Los ciudadanos y residentes estonios obtienen una ID Digital que les permite tener todos los servicios públicos y electrónicos de Estonia, además de que les facilita el establecer una empresa de confianza en la Unión Europea con todas las herramientas necesarias para realizar negocios a bajos costos.

El desarrollo digital de Estonia ha tenido grandes progresos, además de que representa, a escala, las ambiciones de la Unión Europea. A partir de estas transformaciones, y los problemas a los que se han enfrentado, Estonia se ha convertido en un líder tecnológico dentro de la UE. Sus proyectos a futuros involucran el mejorar los servicios que ya ofrecen, además de desarrollar estrategias que faciliten la protección de su ciberseguridad. Después de 2007, Estonia se propone ser el líder en tecnología de la Unión Europea. Busca prevenir los errores del enfrentamiento que tuvieron con Rusia en 2007, además de ser los primero en promocionar el Manual de Tallin para el mejoramiento de la ciberseguridad en la Unión Europea.

[152]Editorial (2016), ¿Qué es Blockchain, la tecnología que viene a revolucionar las finanzas?, *INFOTECHNOLOGY,* Recuperado de: https://goo.gl/7ZRMiu

3.1.2 El recuerdo soviético: recapitulación del Conflicto

> *Las causas de cualquier conflicto bélico radican en los errores y los desaciertos cometidos durante la época de paz. Hay que buscar sus raíces en la ideología de la confrontación y el extremismo.*
>
> *Vladimir Putin*[153]

El dominio soviético en Estonia representó, para los estonios, a diferencia de lo que se cree, una parte oscura en su historia. Tras su liberación de los nazis, el ejército rojo impuso su dominio en las repúblicas bálticas de forma represora. Varios estonios, que estaban en contra del dominio soviético, fueron enviados a Siberia y muchos otros, para evitar el destierro, salieron del país buscando mejores oportunidades en otras partes del mundo.

Cuando Estonia logró su independencia, todo el resentimiento sobre el dominio soviético fue representado en políticas estrictas respecto a quiénes podían tener la ciudadanía estonia, asimismo, la discriminación que sufre la minoría rusa en el país báltico que representa "una tasa de paro (9,7%) que dobla la de la mayoría estonia y que no tienen representación acorde a sus números en los puestos de responsabilidad social o en los mejor remunerados"[154]. De igual forma, esta represión contra la comunidad rusa se daba por influencia que aún Rusia mantenía en el país báltico. La entrada a la UE y a la OTAN fue una forma de desapegarse más de la influencia rusa.

Pese a ello, Rusia no quería perder esta influencia con Europa, además que para la Unión Europea, el adherir a Estonia, no representaba una opción viable. Al tener una cercanía con Rusia, y una influencia cultural muy fuerte, podía afectar en el objetivo que siempre ha tenido Europa de mejorar las relaciones con Rusia. Fue la intervención de Alemania, los países escandinavos y todos los que colindan con el mar Báltico quienes apoyaron la *quasi* membresía de Estonia, junto con Letonia y Lituania, pero al final ninguno aceptó pues querían todos los beneficios de pertenecer a la UE y la OTAN, además de eliminar la influencia de Rusia.

---

[153] RIA Novosti (9 de mayo de 2007), Putin: El 9 de mayo es una fiesta de enorme trascendencia moral, *Sputnik News.* Recuperado de: http://goo.gl/z9qfhP

[154] Herzog, Stephen (2011), Revisting the Estonian Cyber Attacks: Digital Threats and Multinational Respons, *Journal of Strategic Security,* (No. 2), p. 51.

Por su parte, cuando Rusia supo de las intenciones de Estonia por unirse a la UE y la OTAN, utilizó las violaciones a los derechos humanos de la comunidad rusa en territorio estonio para evitar que se tomaran en cuenta los deseos de Estonia. Pero debido a la debilidad económica y política de Rusia tras la desintegración de la URSS, la necesidad de abrir su mercado a occidente y la aceptación al nuevo cambio mundial, tuvo que aceptar todas las presiones internacionales que tenía y dejó de lado el tema de la inclusión a la UE de los países bálticos.

En 1993, en el Consejo Europeo que tuvo lugar en Copenhague, se abren las oportunidades para Estonia, junto Letonia y Lituania. Se les aceptará como miembros de la Unión Europea, para ello se deben cumplir los criterios del Tratado de la Unión Europea, como crear instituciones democráticas que facilitaran los requisitos y además de reducir la agresividad de sus políticas anti-rusas. Para 1999, Estonia ya se presentaba como un candidato fuerte frente a sus homónimos, Letonia y Lituania. Es para 2004 cuando los países bálticos son aceptados en la Unión Europea. Con ello, los beneficios para la seguridad de Estonia aumentaron, pues no solo formarían parte de la UE sino también de la OTAN. Así se lograría reducir la amenaza rusa y por fin comenzar a reunificarse con Europa Occidental.

El objetivo de Estonia, desde este momento, era eliminar cualquier relación que se tuviera con Rusia y con la unión a estas dos instituciones lo lograría. Aunque aún mantiene relaciones por electricidad, transporte, comercio y hasta cultural, lo que busca es descentralizar sus intereses de Rusia y alejarse de sus relaciones con el país de manera diplomática. Para ello, las políticas de segregación contra la cultura rusa son más fuertes y buscan eliminar cada residuo de Rusia. Las políticas contra las minorías rusas son un primer paso y después son los monumentos erigidos a nombre del recuerdo soviético.

El 25 de abril de 2007[155], el gobierno de Estonia, desmantelara y trasladara el monumento que fue construido en la capital del país en honor a los soldados soviéticos caídos en la Segunda Guerra Mundial: *El Soldado de Bronce*; y los 13 cuerpos de héroes soviéticos, lo que produjo una serie de

[155] Justo a unos días antes de los festejos del día de la Victoria en Rusia.

inconformidades y una fuerte división en la sociedad estonia. Esta remoción provocó "un estallido callejero entre el 26 y el 28 de abril que costó una vida en circunstancias poco claras, importantes destrozos en el centro de una ciudad que nunca había vivido semejante experiencia"[156].

Respecto al Soldado de Bronce, fue trasladado a un cementerio militar fuera de la ciudad de Tallin. "El monumento representaba las diferencias entre las dos comunidades del país: para los rusos, el Soldado de Bronce representa la heroica lucha de la URSS contra Hitler y la liberación de Estonia del nazismo; para los estonios, el poder ocupante durante medio siglo y el aplastamiento de Estonia por el terror rojo"[157]

La comunidad judía también apoyó a los rusos debido a que fue el ejército soviético el que liberó a Estonia de los nazis y las víctimas de estos, en su mayoría judíos. "Para el Centro Simon Wisenthal de Jerusalén, el desplazamiento del Soldado de Bronce es un insulto a las víctimas del nazismo"[158]. Esta misma comunidad sentenció que Estonia ha sido indiferente ante los colaboradores estonios del nazismo, lo que produjo una queja mayor contra el gobierno Estonio y huelgas en la embajada Estonia en Moscú por parte de ciudadanos rusos. Aun así el gobierno ruso no pudo hacer algo al respecto de forma directa pues estaría entrometiéndose en un país soberano; aunque los discursos políticos y acciones que tomaría después harían notar el apoyo a la minoría rusa de aquel país.

3.1.3 El ataque DDoS que desestabilizó a Estonia

> *Cuantos procuran minimizar la experiencia inapreciable de los veteranos y profanan los monumentos a los héroes de la guerra, faltan el respeto a su propio pueblo, traicionan la memoria histórica, siembran discordia y desconfianza entre los Estados y entre la gente*
>
> *Vladimir Putin, 9 de mayo 2007. Discurso proclamado el día de la Victoria haciendo referencia a los acontecimientos recientes en Estonia*[159]

[156] Martínez de Rituerto, Ricardo (7 de mayo de 2008), El militar de bronce que divide Estonia, *El País,* Recuperado de: http://goo.gl/5uHiJF
[157] *Ídem.*
[158] *Ídem.*
[159] RIA Novosti (9 de mayo de 2007), Putin: El 9 de mayo es una fiesta de enorme trascendencia moral, *Sputnik News,* Recuperado de: https://sptnkne.ws/g4G2

La mañana del 1º de mayo del 2007, Estonia amaneció con problemas en la red informática de todo el país. Los primeros ataques fueron en la sustitución de portales oficiales del gobierno donde se agregaron imágenes insultantes para el primer ministro estonio. Aunque en las primeras horas del día no había muchos incidentes respecto a la red no se tomaron precauciones hasta que comenzaron a colapsar más redes: de comunicación, bancarias, de gobierno.

Fueron unas horas después cuando el tráfico en internet se disparó bruscamente hasta saturar los servidores y hay colapso de las mismas, la población comienza a ser afectada. Unas horas después ya no había información, las pantallas de las computadoras se quedaron en negro. Las agencias de noticias y los dos bancos comerciales más importantes de Estonia se habían desconectado. Asimismo, todos los servicios en línea se suspendieron y esto comenzó a generar desesperación en la población pues no sabían lo que estaba ocurriendo y si tardaría en solucionarse. Su vida era dependiente de todas las redes colapsadas.

La comunidad rusófona continúa con las huelgas contra el gobierno y sus políticas de segregación[160] en la parte céntrica de Tallin. Mientras tanto los sistemas informáticos están siendo bloqueados. Los servicios cotidianos, como la distribución de la gasolina y el pan, son suspendidos. Las autoridades comienzan a tomar acción tanto contra las revueltas como dentro del sistema informático. La presión aumenta al punto que ya no solo son los rusos que están en revueltas contra el gobierno sino los propios estonios se unen ante la incompetencia del gobierno por otorgarles sus servicios básicos y temer que su información personal (seguros de vida, datos personales, servicios bancarios) quedase vulnerada[161].

Tras varias horas de tratar de recuperar los servicios, comienzan buscando el origen del ataque. Los estrategas estonios buscan una solución en la red pero el origen del ataque es muy disperso porque se identifica, primero en Rusia, pero después identifica a más países donde se originan los ataques como Francia, Inglaterra, Italia, Alemania y hasta proveniente de los Estados Unidos. El no saber de dónde provienen los ataques, comienza a crear un caos. Entonces identifican el tipo de ataque que están sufriendo, es un

[160] Ya eran dos noches seguidas en que las huelgas habían estallado y habían provocado saqueos.
[161] GEDEON (1 de junio de 2013) Ciberguerrilla, *GEDEON,* Recuperado de: https://goo.gl/Xbs3mu

Distributed Denial of Service (*DDoS*) o Ataque Distribuido de Denegación de Servicio.

Este ataque consiste en "crear muchas conexiones simultáneas o enviar paquetes alterados […]. También permiten modificar los paquetes poniendo como IP de origen una IP falsa, de forma que no pueden detectar quién es el atacante real"[162]. El ataque utilizado en Estonia es un derivado que consiste en "usar *botnets*: redes de ordenadores infectados por un troyano y que un atacante puede controlar remotamente. De esta forma, los que saturan el servidor son ordenadores de gente que no sabe que están participando en un ataque *DDoS*, por lo que es más difícil encontrar al verdadero atacante"[163]. La única alternativa que encontró el gobierno estonio fue la desconexión total con el mundo para impedir que el ataque fuese más fuerte y realmente los dejará totalmente vulnerables.

Las Infraestructuras Críticas estuvieron vulneradas ante un ataque no previsto. La debilidad de Estonia, y de la respuesta de la Unión Europea, fueron mostradas en un ataque que solo buscaba causar daños como parte de un conflicto que pudo terminar con todas las IC de Estonia y quizá dañar, de manera más grave, la composición del país. Y aunque el conflicto no tuvo problemas a largo plazo, si despertó la inquietud de la Unión Europea, la OTAN y de la comunidad internacional. Este ya no era un conflicto de virus informático o entorpecer comunicaciones, era un ataque directo a las estructuras más importantes para el Estado. Un problema común a resolver.

3.1.4 Las medidas de Estonia y la colaboración internacional

Como miembro de la Unión Europea y la OTAN (ambos en 2004), Estonia buscó el apoyo de ambos actores para la solución de su problema informático. La respuesta que obtuvo fue "la colaboración de equipos internacionales de respuesta a emergencias en internet, así como de servicios de seguridad de otros gobiernos expertos en ciberdelincuencia y ciberterrorismo"[164]. Los

[162]Guillermo Julian (2 de febrero de 2012), "¿Son los *DDoS* efectivos como medios de protesta?", *GENBETA,* Recuperado de: http://goo.gl/uwrdOh
[163]Ídem.
[164]Martos , José Ángel (9 de noviembre de 2014), ¡Esto es la Ciberguerra!, *Muy Interesante,* Recuperado de: http://goo.gl/DFowA6

primeros informes que se le proporcionaron no complacieron a Estonia pues no localizaban a un culpable seguro, tuvo que presionar a los equipos de apoyo para que encontraran al culpable. Al final el único culpable factible fue Rusia, pese a que el ataque se localizó en muchas otras partes del mundo.

El ministro de defensa estonio, Jaak Aaviksoo, sentenció que era un asunto de gravedad y "culpó directamente a Rusia respecto al asunto pues había varias pruebas que condenaron el apoyo del gobierno ruso. Pues las oleadas de ataques tuvieron lugar de acuerdo con la hora de Moscú"[165], además de que los expertos detectaron que la mayoría de los ataques provenían de Rusia, y que el evento informático fue justamente después de los conflictos con la minoría rusa en Estonia. Además que, durante los días que duró el ataque, el presidente Vladimir Putin hizo un hincapié en los acontecimientos de Estonia, sin mencionar lo del ciberataque, defendiendo como siempre a la comunidad rusa y castigando los actos contra esta por parte del gobierno estonio.

Las herramientas cibernéticas utilizadas para el ataque no podrían haberse desarrollado sin un fuerte financiamiento, como el que podría proporcionar un gobierno:

> En Estonia, el 97 por ciento de las transacciones bancarias se producen en línea; y en 2007, el 60 por ciento de la población del país utiliza Internet sobre una base diaria. Estonia es tan dependiente de Internet que su modelo de operaciones del gobierno se conoce como *gobierno sin papel.*[166]

Las pérdidas que tuvo el gobierno de Estonia fueron en su mayoría económicas, uno de sus bancos estimo que "sus pérdidas operativas debido a las huelgas fueron alrededor de 1 millón dólares en daños, además de que los ataques impidieron las transacciones con tarjetas de crédito y cajeros automáticos". Asimismo, los piratas informáticos desactivaron el servidor de correo electrónico "y las capacidades de comunicación en varios ministerios del gobierno, paralizando la capacidad del estado para responder eficazmente"[167].

---

[165] *Ídem.*

[166] Herzog, Stephen (2011), Revisting the Estonian Cyber Attacks: Digital Threats and Multinational Respons, *Journal of Strategic Security,* (No. 2), p. 52

[167] *Ídem.*

Al final, no se pudo culpar al gobierno ruso, aunque había algunas pruebas, no eran suficientes para declararlo el organizador del ataque y solo se enjuicio a un chico[168] al cual jamás se le castigó.

El apoyo que tuvo Estonia para defenderse de estos ataques fue principalmente por parte de Estados Unidos quién catalogó de ciberterrorismo los ataques ya que desestabilizaban totalmente la capacidad de un país para funcionar en plenitud. “Los piratas secuestraron computadoras, incluyendo muchos PCs para el hogar en lugares como Egipto, Rusia y los Estados Unidos y los utilizaron como *enjambre*”[169] dentro del sistema informático estonio.

El Internet, como medio, se ha convertido en una herramienta poderosa para “coordinar grupos transnacionales que se ven a sí mismos como marginados, y tratan de intimidar a los Estados-nación y otros agentes presuntamente responsables de sus quejas”[170]. Después de esta experiencia, Estonia, buscó renovar su seguridad cibernética para prevenir un ataque similar. Su objetivo fue transformarse en el país con un mayor avance tecnológico respecto a la ciberseguridad y ser el país que sirva de base para las políticas de seguridad y defensa en el ciberespacio que se planteará en el futuro la Unión Europea.

3.2 Repensar la ciberseguridad

Si reconsideramos la situación y los eventos ocurridos en el 2007, el ataque apenas fue una muestra del desastre que pudo ocurrir en Estonia. El ciberataque tuvo repercusiones en el comercio, servicios públicos y operaciones del gobierno. “En futuros ataques, los hackers pueden ser orientados al abastecimiento de agua, redes eléctricas, controles de tráfico aéreo, o incluso sus sistemas de armas militares [sic].”[171] Este caso conmocionó a la comunidad internacional y dejó claro que tenía que existir una solución, o una regulación, a este tipo de crisis.

La gravedad de los ataques a Estonia generó una respuesta internacional rápida. “Estonia tenía pocas preparaciones formales en

[168] El chico pertenecía a un grupo Neo-nazi en Rusia
[169] Herzog, Stephen, Op. Cit., p. 52
[170] *Idem*
[171] *Ibid. P. 54*

ciberdefensa fuera de su marco para la lucha contra los actos de terrorismo tradicionales, el *Computer Emergency Response Team* (CERT) requirió de la asistencia de los gobiernos de Finlandia, Alemania, Israel, Eslovenia y de la OTAN para restablecer las operaciones en red"[172]. Además de que la Agencia de Seguridad y Red de Información Europea (ENISA) ofreció asistencia técnica de expertos para apoyar en el desarrollo de los hechos y contrarrestar los ataques a través de las redes digitales.

Es justo después de los ataques *DDoS*, que los estados miembros de la OTAN y la UE "comenzaron a debatir sobre las nuevas orientaciones de la seguridad cibernética y las sanciones correspondientes de los estados que hayan participado, o participen, en la guerra digital. Las sanciones son una opción castigo recibieron un apoyo bastante generalizado"[173] Y estas son plasmadas en algunos artículos del Manual de Tallin publicado en 2013.

Alemania propuso ampliaciones al artículo 5 de la OTAN en lo que se refiere al apoyo en ciberdefensa que es aceptada en abril de 2008. Esta ampliación busca la cooperación por parte de todos los países miembros para enfrentar situaciones similares en un futuro. En ese mismo año, se crea la base *Cyberdefence Management Authority* (CDMA) en Bruselas que tiene como objetivo "centralizar las capacidades operativas de defensa cibernética a través de la Alianza"[174]. Ya en agosto de 2008, "Tallin se convirtió en la sede del *Centro de Excelencia para la Ciberdefensa Cooperativa*, que resguardará la seguridad cibernética de la Alianza Atlántica"[175].

Todos estos nuevos mecanismos de ciberdefensa comenzaron a poner a Estonia en un papel protagonista para los miembros de la UE como primer país que desarrollaban, de manera avanzada, estrategias para la ciberdefensa. Estonia comprometió a diversos países a la participación en el Centro de la OTAN y a trabajar en conjunto tanto para la OTAN como para la UE. Las relaciones tan críticas con Rusia han hecho que Estonia se capacite en la ciberdefensa y pueda promoverla en el resto de sus homólogos.

---

[172] *Idem*
[173] *Ibid.,* p. 55
[174] *Ídem.*
[175] Ministerio de defensa (2011), Nuevo concepto de ciberdefensa de la OTAN *Instituto Español de Estudios Estratégicos,*(No. 9), p. 3

Ya a lo largo de 2010 y principios de 2011, la UE y la OTAN anuncian una serie de planes concretos a largo plazo encaminados a contrarrestar los ataques cibernéticos. La *Agenda Digital de la Unión Europea* trazó, en aquel momento, planes para "establecer protecciones en sus instituciones, mantener simulaciones en ciberdefensa multinacionales, y crear una plataforma conjunta contra el cibercrimen"[176]. En cuanto a la OTAN, buscó desarrollar fuertes capacidades de defensa en Internet y se crea el *Computer Incident Response Capability Technical Centre* (que entró en funcionamiento en 2012).

El evento cibernético representó, para todos los actores involucrados, una transformación en este ámbito. Por un lado, un preventivo para las Infraestructuras Críticas totalmente vulnerables, que aunque se trabajaba en resguardarlas, fueron el primer blanco para el ataque. Como segundo punto, el planteamiento de una estrategia de ciberseguridad decente pues Rusia, anteriormente, había sido blanco de un ciberataque. Si realmente fue Rusia quien lo atacó, es posiblemente que haya sido una prueba tanto para saber con qué cuenta el enemigo como qué tan efectivas son sus propias armas cibernéticas.[177]

El primer ataque, de este tipo, que recibió Rusia, fue en 1980 en sus sistemas de gasoducto tras robarle a la CIA un sistema informático que fue sido modificado con anterioridad. Se instaló en el sistema que controlaba los yacimientos de gas de Urengoi, que era la construcción más importante para la Unión Soviética[178]. El sistema informático provocó la explosión de los tubos de gasoducto produciendo un gran desastre y pérdidas económicas. No fue un fallo técnico sino una cuestión de espionaje. Un agente doble, que trabajaba para Estados Unidos en realidad, llevó a la URSS el sistema informático para el gasoducto y tras la violación del sistema, hubo un fallo. Para Rusia fue el primer paso para mantenerse al margen de los desarrollos de occidente e ir a la par en lo que refiere a ataques cibernéticos. Es por ello que busca mejorar

[176] Abadal, Ernest (2011), Agenda digital europea: las cosas que se deben hacer para mejorar en TIC en Europa, *Blok de bid*, Recuperado de: http://goo.gl/dW6dlH

[177] Un enemigo elegido al azar y gracias a los problemas que sus relaciones políticas representaban en ese momento.

[178] Cid, Ana Teresa (2008), El rescate de la industria petrolera en Rusia, *SCIELO*, vol. 21 (Num. 58), recuperado de: https://goo.gl/Jsw5Ci

sus propias capacidades de ciberguerra y estrategias a comparación de occidente.

El ciberataque se convirtió en un ultimátum respecto a las políticas contra la comunidad rusa que disponía el gobierno Estonio. Y sirvió como una alerta para el mundo pues "en el futuro, habrá una mayor atención a la seguridad cibernética y las nuevas estrategias e instituciones multinacionales jugarán un papel decisivo en la lucha contra las amenazas informáticas"[179] que atenten contra la soberanía y la supervivencia de los estados. Y evitar que se anime a futuros grupos criminales, o no criminales, a volver a realizar actos de este tipo pero con un mayor impacto a nivel internacional.

Fue el ingrediente necesario para que la Unión Europea comprendiera la importancia del ciberespacio y la seguridad. Plantearía nuevas posibilidades a sus aliados más cercanos y comenzaría una discusión, a nivel internacional, sobre lo que es o no necesario plantear en este nuevo tipo de guerras. Si bien, se han creado mecanismos de prevención, es evidente que no solo eso es necesario para poder establecer un orden con lo que se refiere a ciberespacio. Ya no son suficientes los análisis a partir de lo que ya se tiene sino se necesita repensar en otros mecanismos viables para una verdadera efectividad. El gran reto de este nuevo pensamiento a la seguridad será el planteamiento de escenarios futuros viables y la forma de actuar en ellos.

3.3 La creación del Manual de Tallin: Retos y oportunidades

La creación del Manual de Tallin sobre el Derecho Internacional Aplicable a los Conflictos Armados Cibernéticos [o Manual de Tallin o Manual] es una iniciativa que estaba tardando en ser propuesta. No solo porque los acontecimientos con Estonia movieron la dinámica internacional con respecto a los ciberconflictos. Sino que ya otros países se venían enfrentando a este nuevo tipo de desafíos y no habían sido conceptualizados con tanto esmero. Es la primera vez que realmente se unen diferentes actores (países, organismos, empresas, etc.) para resolver las problemáticas que trajo el ciberespacio.

El Manual es un compendio de leyes sobre el ciberespacio creado por expertos en el tema pertenecientes a diferentes instituciones. Este Manual aún

[179] Herzog, Stephen; Op. cit. p. 56

no tiene relevancia legal pero podría representar un primer antecedente a una legislación internacional sobre la ciberguerra, y el ciberespacio en general. El Manual se crea a partir de los acontecimientos de Estonia en 2007 pues fue un evento invasivo a través del ciberespacio que demostró las debilidades de un país tan avanzado en tecnología.

La base para la constitución del Manual de Tallin es a partir de los tratados más relevantes sobre guerra. Se recogen las implicaciones del *Ius ad Bellum,* donde se limita el recurso de la fuerza para los Estados con el propósito de cumplir lo acordado en la Carta de Naciones Unidas, y del *Ius in Bello, que* consiste en regular la forma en que se conducen las hostilidades a partir de lo humanitario. Todo esto consisten retomar las cuestiones de guerra para poder aplicarlas al ciberespacio, en específico a los ciberataques (o en el caso de una ciberguerra, las ciberoperaciones).

Debido al desarrollo tecnológico del que depende Estonia, el pensar en una estrategia de seguridad era evidente. La cuestión es que no estaba preparada antes de los ataques de 2007 y el daño fue inevitable. De esta experiencia no solo comprendió la necesidad de una estrategia de seguridad, sino que buscó ser el primero en fomentar la ciberseguridad en toda la UE de forma rigurosa. No quería que solo se plantearan directivas como en el Consejo Europeo se había propuesto, donde los intereses tanto de los miembros como de sus socios comerciales o políticos no se vieran afectados, sino que tuviera una verdadera eficacia. Es por ello, que cuando se establece el Centro de Excelencia en la Defensa Cooperativa Cibernética de la OTAN en la capital estonia (Centro de Excelencia), es Estonia que comienza a presionar para la creación de un instrumento legal que funcione para prevenir y castigar este tipo de sucesos, no solo a nivel nacional sino en toda la Unión Europea.

En 2009, el Centro de Excelencia reúne a un grupo de expertos en el área legal, algunos eran expertos en la cuestión cibernética por práctica. Tanto investigadores como expertos profesionistas se enfocan en crear un manuscrito de cómo debe ser interpretado, en el derecho internacional, las ciberoperaciones y la ciberguerra. Se buscaba examinar, de forma exhaustiva, los vacíos legales que existen respecto al tema. Y desarrollar un instrumento que funcione como base o como ejemplo de lo que podría hacer el Estado si llegase a ser víctima de estas ciberoperaciones.

Tabla 10. Grupo de Expertos		
Representación	**Institución que representan**	**Experto**
Estados Unidos		Michael N. Schmitt (Director del Proyecto)
	Brigham Young University	Profesor Eric Talbot Jensen
	Creighton University	Profesor Sean Watts
	University of Potsdam	Profesor Robin Geiss
	University of Texas	Profesor Derek Jinks
	United States Naval Postgraduate School	Profesor James Bret Michael
Europa	Viadrina European University	Profesor Wolff Heintschel von Heinegg
	United Kingdom Royal Air Force	General de Brigada Aérea (retirado) William H. Boothby
	Chatham House	Dr. Louise Arimatsu
	George C. Marshall European Center for Security Studies	Profesor Thomas C. Wingfield
	Catholic University of Leuven	Bruno Demeyere
	* University of Amsterdam * Netherlands Defence * Academy Utrecht University	Profesor Terry D. Gill
	Swedish National Defence College	Profesor Jann Kleffner
	Geneva Centre for Security Policy	Dr. Nils Melzer
Canadá	Canadian Forces	* Capitán Naval Geneviève Bernatchez * Kenneth Watkin
Australia	Australian Defence Force	Coronel Penny Cumming
OTAN	NATO Cooperative Cyber Defence Centre of Excellence.	* Dr. Kenneth Geers * Dr. Rain Ottis
Fuente: OTAN (2007), Tallinn Manual: Panel of Experts, *Cooperative Cyber Defense of Excellence*, Recuperado de: https://goo.gl/rR3SSm		

Este grupo (*Grupo de expertos*) es liderado por Michael N. Shmitt, presidente del departamento de derecho internacional del Colegio de Guerra Naval de los Estados Unidos[180]. Otros miembros del grupo pertenecen a

[180] Se supone que ninguno de los participantes en la creación del Manual quieren que aún se convierta en un instrumento jurídico y se escuda que es solo un Manual de referencia sobre lo que podría hacer un Estado ante un *ciberataque* (todas las conferencias que hablan del Manual lo repiten los representantes de la OTAN), sin embargo el interés porque se siga renovando año con año (de ahí que saldrá la versión del Manual 2.0 enfocado en las ciberoperaciones) es plantear ya un interés porque realmente el Estado pueda controlar este espacio al cual no se ha podido controlar en su totalidad. Tal vez la ciberografia se convierta en un ciencia del mañana que proporcione a este Manual la oportunidad de ser factible al ya poder trazar un mapa de lo que es el ciberespacio. De no ser así, no serían tantas instituciones y gobiernos interesados en todo lo que se escribe en este Manual.

Europa, de los países que pertenecen a la OTAN, Canadá, Australia, además de organismos como Comité Internacional de la Cruz Roja, que vigilaba el que se respetara el Derecho Humanitario, y el cibercomando de los Estados Unidos. Los nombres de los representantes se encuentran desglosados en la **tabla 9.**

Para su elaboración, se tomaron como base el Manual de San Remo sobre el Derecho Internacional aplicable sobre los conflictos armados en el mar [1994] y el Manual sobre el Derecho Internacional aplicable para el aire y la guerra de misiles. El Manual se divide en secciones o reglas (que están en letras negras) junto con un comentario respecto al censo al que llegó el Grupo de Expertos sobre el tema a tratar. Hay que recordar que el Manual no es una visión oficial sobre los actores participantes, es solo la visión del grupo de expertos sobre las cuestiones de ciberguerra[181].

El posicionarse en una doctrina a seguir implicaría muchas responsabilidades que ningún actor quiere contraer aún, mucho menos cuando el Manual ha causado demasiadas controversias con respecto a los artículos propuestos. El Manual se debe considerar como un debate de lo que podría ser la legislación de la ciberguerra y en las posibilidades que tiene un Estado en un enfrentamiento de este tipo. El debate continua siendo constante, pues ya existen 2 versiones del Manual que retoman las cuestiones de la legalidad de la ciberguerra y no parece ser un trabajo que concluya con la última versión pues, al igual que el espacio que se está estudiando, es un constante cambio y necesita ser reestudiada.

A diferencia del resto de los espacios físicos, el ciberespacio es creado a partir de la guerra, un instrumento para la guerra y no un espacio donde combatirla. El desarrollo tecnológico cambio su propósito y su popularidad aumentó de modo que se consideró como un medio de revolución por la idea utópica de que no lo gobierna nadie más que quienes ahí lo “habitan”. El ciberespacio, para la visión de las personas, no es un gobierno multilateral de los Estados sino un gobierno a partir de todos los actores que lo conforman. Si

[181] Hago hincapié en esta idea de que no es un instrumento jurídico, aún, porque así lo han hecho ver todos los participantes, en especial la OTAN, que al ser un organismo de seguridad militar no quiere tomar una posición con respecto a lo dictado dentro del Manual de Tallin.

un gobierno estatista se hubiera adueñado de lo que es el ciberespacio, seguramente no representaría la revolución que representa en nuestros días.

Aún así, el ciberespacio debe tener cierta injerencia del Estado. La regulación que tiene el mismo se ha logrado gracias a sus actores pero también a instituciones que han sido apoyadas por el mismo gobierno y las infraestructuras que permiten, a las personas, entrar al ciberespacio a través de internet. Es por ello, que aunque se quede el ciberespacio como un elemento utópico de revolución, la injerencia del gobierno es importante, un poco necesaria aunque al final es posible que el propósito se desvié de las responsabilidades reales que debe tener el Estado. El mismo Manual de Tallin lo plasma al darle más responsabilidades al Estado con respecto al ciberespacio y la ciberguerra. El Manual tiene el objetivo de crear un debate a partir de la necesidad de modificar el Derecho Internacional para que pueda ser aplicable al ámbito del ciberespacio. El Manual se conserva como una guía a los posibles ataques que pueden presentarse a los Estados.

El Manual se constituye a partir de dos leyes en el que cada una enlaza diferentes intereses. El primero es sobre las leyes cibernéticas y el Estado, la segunda es sobre las responsabilidades en los ciberconflictos armados, en este se retoman cuestiones a partir de las personas, Infraestructura y el Derecho Internacional Humanitario. Estas leyes se abordarán de forma muy técnica para conocer el contenido de las mismas, su constitución y los aspectos más relevantes de cada sección.

3.3.1 Primera parte: Ley de seguridad cibernética

Esta primera parte desarrolla las cuestiones primordiales a tratar por parte de los Estados respecto a la responsabilidad, soberanía, control, jurisdicción, acciones internacionales, defensa y uso de la fuerza. Se aborda a partir de que un Estado será el responsable en todas las cuestiones de ciberseguridad pues, aunque ya no es el actor central de la dinámica internacional, si representa el sujeto que debe mantener la seguridad de sí mismo como parte de una obligación jurídica.

El primer tema a desarrollar es el principio de soberanía. Este ha sido rector de las relaciones jurídicas en el Derecho Internacional. Estas relaciones

jurídicas perfectamente pueden seguir en las cuestiones del ciberespacio. En especial, cuando se habla de infraestructuras críticas que competen a la conectividad del ciberespacio. El Manual de Tallin plantea que existen dos responsabilidades respecto a la soberanía del Estado. Primera, las infraestructuras críticas dentro del territorio solo pueden tener control regulatorio el Estado. Segunda, es el Estado el responsable de proteger dichas infraestructuras.

La relación entre Estado, Infraestructuras Críticas y ciberoperaciones es muy importante para la aplicación del derecho internacional tanto en tiempos armados como en tiempos de paz. Se debe reiterar la importancia de la soberanía de los Estados y la responsabilidad que esto conlleva. Es complejo comprender desde qué punto un ciberataque puede ser autoría de un Estado pero esta parte solo recalca que las ciberoperaciones, por parte de los Estados contra las IC localizadas en otros Estados, son acto contra la soberanía.

En esta primera parte no se le obliga a los Estados a crear medidas preventivas que eviten los ataques debido a lo complejo que es detectarlos pero tampoco establece un criterio que pueda ser la base para determinar medidas que prevengan estos ataques. Además de no plasmar mecanismos que ayuden a comprender cuando un ciberataque es de un gobierno, y no de otro actor. Esto conlleva a algunas problemáticas importantes que no son plasmadas en el Manual[182]:

- La gravedad del daño que debe causar un ciberataque que obligue al Estado a intervenir
- El tipo de ciberataques que se le pueden atribuir a un Estado
- Las sanciones que debe imponer el Estado

Como se explica en el capítulo 1, los ciberataques tienen diferentes características que lo componen, además de que cualquiera puede hacerlo funcionar. La debilidad del Manual radica en el momento de definir al responsable de los actos y con qué instrumentos se le permite a un Estado identificar el origen del ataque. Ya que se deja al criterio de los países podría

[182] Vázquez Ortiz, Ana Pilar (2016), Principios del Derecho Internacional aplicables a la acción de los Estados en el ciberespacio. Mando Conjunto de Ciberdefensa. *Jornadas de Ciberdefensa 2016* Recuperado de: https://goo.gl/rpehcr

involucrar muchas violaciones a la privacidad tanto de otros países como a civiles. Si no se otorgan criterios concretos, o por lo menos que orienten al país atacado, a descubrir al atacante cualquier método puede ser usado para ello y termine siendo perjudicial.

Relacionado con ello, la distinción entre actores atacantes y sus consecuencias no definidas. No se especifica qué tipo de actor puede pertenecer al Estado. Por ejemplo, una empresa que esté trabajando para un Estado en un ciberataque contra un segundo Estado. En este caso, no existe un acuerdo de dónde podría catalogarse y cómo podría sancionarse pues el autor del ataque no es gubernamental pero si está trabajando para uno. O en la cuestión de los civiles, se justifica el enfrentar al enemigo, sea civil o no, como enemigo de guerra.

Esta cuestión nos brinda demasiados aspectos a discutir. El primero, la forma en que se enjuicia a un culpable civil. Si fuese en un juicio de guerra, esto permitiría seguir las normas de un Tribunal Militar y no tendrían los privilegios de un civil, si se diera el caso. Siendo enemigo de guerra y atentando contra una nación, se castigará hasta las últimas consecuencias. A partir de esta situación, surge la cuestión de la viabilidad de llevar un caso a un juicio de guerra, tal vez a un tribunal militar. Si en el acto se perdió dinero o se ocasiono algún otro suceso ¿qué tan viable es enjuiciar a un civil y encerrarlo en una cárcel militar? Al final las consecuencias tienen que representar una verdadera sanción que demuestre la capacidad del Estado atacado pero si se mantiene al culpable en una prisión, no queda claro el efecto que al final tendría en el ciberespacio.

De igual manera, se supone que queda a criterio de cada Estado el buscar la forma de contestar. Tampoco se especifica las características del ataque. Pueden ser similares o más dañinas que el ataque del oponente, tener efectos más devastadores y aún así entra en lo acordad: al criterio del Estado. Es aquí cuando el uso de la fuerza se vuelve un actor clave para comprender los planteamientos del Grupo de Expertos.

En primera, el Manual de Tallin plantea como Arma cibernética: “la capacidad de las acciones cibernéticas para materializarse como un uso de la

fuerza contraria al Derecho Internacional"[183] La cuestión es planteo del todo es sobre cómo y bajo qué circunstancias se puede catalogar como acción armadas. Esto obliga a evaluar si estas acciones, como uso de la fuerza. Es a partir de lo convencional, de uso indirecto o uso agravado de la fuerza.

Debido a que existe el *Efecto reductor de las asimetrías,*[184] que consiste en capacitar a cualquier agente, sea estatal o no, para realizar acciones consideradas del uso de la fuerza, es difícil encontrar al autor de las acciones y de catalogar estas mismas acciones pues no existen características de las cuales partir para considerarlas como uso de la fuerza contra un Estado.

Con esta idea podemos retomar la idea de los cibersolados, como se menciona en el libro *Cyberpunks* de Julian Assange. Personas capacitadas para la ciberguerra a partir de los principios de los entrenamientos militares. Si bien, en muchos ciberataques existe evidencia de que la autoría no fue de un Estado sino de una empresa o de un actor civil, al ya contar con un ciberejército esto podría proporcionar patrones para conocer los tipos de ciberataques a enfrentar o tal vez complique, en mayor medidas estos mismos. Si se tiene un ciberejército propio, es más fácil un ciberataque de Estado a Estado, pero también se tiene que conocer qué estrategias, técnicas o elementos pueden diferenciar un ejército estatal de un actor individual. Además, los criterios de sanción serían diferentes porque ya existiría un atacante civil y uno militar.

Tanto la soberanía como el uso de la fuerza es difícil plantearlos a partir de las premisas presentadas en el Manual de Tallin pues al final es el Estado el sujeto más importante. El problema principal será la definición de los actores respecto a las acciones llevadas a cabo. Además de que se necesitan ampliar varios conceptos que puedan ser más perceptibles en los temas de ciberataques. Si realmente se quiere tener un orden, a partir del Estado, es necesario crear acuerdos interestatales que permitan reforzar sus capacidades en el área cibernética para imponer su autoridad y legitimidad sobre estos asuntos.

---

[183] *Ídem*

[184] Robles Carrillo, Margarita (2016), Uso de la fuerza en el ciberespacio: las armas cibernéticas. Mando Conjunto de Ciberdefensa. *Jornadas de Ciberdefensa 2016* Recuperado de: https://goo.gl/rpehcr

La cuestión de esta primera parte es la definición de actores y la soberanía del Estado. Al igual que en el mundo físico, el Estado puede usar sus infraestructuras (en este caso ciberinfraestructuras) como quiera sin afectar las de otro Estado. En el ciberespacio, este es un problema al momento de delimitar fronteras, en el caso de las IC conectadas al ciberespacio. Y saber si estos ataques tienen efectos en la Infraestructura física del ciberespacio (los cables submarinos, la fibra óptica, IPS).

El problema en este punto es que no existe un consenso entre el Grupo de Expertos si esa soberanía ha sido infringida o violada en caso de la pérdida de la funcionalidad. No se le especifica a un Estado hasta que nivel tiene que llegar un ciberataque para que pueda intervenir. Si bien, ya solo con atentar contra el Estado es un punto para responder, en la guerra física existen normas que permiten saber a un Estado hasta qué punto puedes responder de la misma manera. El Manual ya habla de una ciberguerra, una intervención con propósitos bélicos que podrían tener consecuencias graves a futuro.

3.3.2 Segunda parte: La ley del conflicto cibernético

Esta segunda parte es el aspecto fundamental de Manual. El *Ius ad Bellum* y el *Ius in Bello*. Se debate sobre las responsabilidades de los Estados en las cuestiones de guerra, es la parte primordial del Manual que estable las reglas de cómo se tiene que llevar a cabo la ciberguerra. Hay que dejar en claro, que pese en esta investigación se plantearon conceptos como ciberguerra o ciberoperaciones, no son aún aceptados, el único aceptado es el ciberespacio y aún así su definición ha sido compleja. Por ende, las premisas con las que trabaja el Grupo de Expertos no son fijas y se basan en los conceptos establecidos en las instituciones que representan. Al final, se traslada la Guerra al ciberespacio[185], y con ello las cuestiones más importantes de los tratados y convenios internacionales recordándonos la dependencia de ambos espacios.

El Derecho Internacional Humanitario es primordial para los convenios y tratados sobre la guerra pues garantiza el cumplimiento de los Derechos Humanos en el mundo. En la Guerra este derecho es importante debido a la

[185] Junto con los conceptos que conlleva.

larga historia de violaciones contra la vida humana. Por ellos son igual de indispensables los Derechos Humanos en las cuestiones de ciberguerra. Aunque parezca que jamás se afectará a una persona, sí existen hechos y casos que podrían violentar la seguridad de las personas.

En el Manual se pretende extrapolar el principio de *Ius ad Bellum* para que las ciberoperaciones sean legitimadas en casos de que se atente contra los Derechos Humanos o las mismas IC de las que dependen las personas. Para este caso tampoco se plantea en el Manual en qué circunstancias o qué tipo de ciberataque se tiene que recibir para considerar usar este principio de guerra. Este es uno de los puntos no explorados para definir un ciberataque.

Para entender un ciberataque se tienen que considerar varios criterios como el tipo, el objetivo, siendo que puede ser atacado un objetivo civil o militar, no se define con exactitud qué se considera como objetivo aceptable; el escenario, en este caso no es un territorio físico como el marítimo, aéreo o terrestre, sino uno inventado por el hombre, el ciberespacio. El enfrentamiento puede ser de carácter mundial por lo que complicaría las cuestiones de localizar a un objetivo o al autor de la *ciberataque*.

El Manual de Tallin habla del principio de neutralidad, que básicamente es no tomar partido o injerencia en los conflictos armados. En el Manual es algo más complejo pues tiene que definir qué países son neutrales en un enfrentamiento cibernético. Se va a castigar si llegase a existir un ataque a una IC perteneciente a un país neutral. Este principio es uno de los principales retos pues se debe definir los países neutrales y las formas en que se identificarían los ciberataques y sus víctimas.

Además de que no retoma el principio de neutralidad de red, que es la transmisión del tráfico de datos en la red de forma indiscriminada. Este principio de neutralidad debería abordarse ya que, aunque varios gobiernos estén de acuerdo con ellos podría violentarse a favor de algún actor. Y debido al anonimato en la red, no existiría una forma factible de hacer cumplir este principio.

Como se puede comprender, el ciberespacio no podría causar daños en lo físico tan directamente como si se atacaran IC, tanto del ciberespacio como del Estado. En estos casos, y no es mencionado en las variables del Manual de Tallin, la cuestión de nuevas armas, como los drones. Su manejo es a

través del ciberespacio y tiene efectos graves en el mundo físico lo cual también debe ser una forma de regulación tanto para el Derecho Físico como el cibernético.

No es la primera vez que un nuevo medio lleva a discusión las cuestiones de enfrentamientos armados. Cuando se inventa el primer avión, era evidente que su uso no solo sería para transportar personas sino que ahora también sería una herramienta muy útil para la guerra. De igual forma, el ciberespacio está trayendo a debate todo este derecho de guerra aplicable al ciberespacio para poder crear verdaderas medidas preventivas que no dejen vulnerable a un Estado pero que tampoco vayan contra las garantías de los derechos humanos.

No es sencillo poder analizar toda la cuestión del Manual de Tallin pero si se combaten estos puntos débiles para la aplicación de cada participante, podría desarrollar políticas de ciberseguridad y ciberdefensa que realmente sean efectivas en aplicación. El problema que radica es la característica del enfrentamiento. Debido a las condiciones del anonimato, la guerra asimétrica es inevitable.

Cualquiera puede ser el enemigo, la diferencia radicará en la cantidad de atacantes y en los recursos que se cuenten para hacerlo. Las reglas convencionales de combate no son aplicables y las aristas son demasiadas para poder establecerse reglas que funcionen. La debilidad más grande de un conflicto de este tipo es el mismo medio en el que se mueve y la misma composición del conflicto.

3.3.3 Retos y campos de acción

El Manual de Tallin representa una gran transformación para la legislación del ciberespacio. Pese que su enfoque está dedicado a la ciberguerra, muchas otras cuestiones nacen o resurgen con lo propuesto por el Grupo de Expertos. Para poder legislar la ciberguerra se necesitan debatir muchas otras características que componen tanto el campo donde se dará este nuevo tipo de enfrentamiento como los elementos que permitirá que ocurra un enfrentamiento así.

El Manual nos presenta dos enfoques sobre las cuestiones del ciberespacio: los retos que se afrontan tanto ahora como en el futuro con respecto al ciberespacio y sus lagunas legislativas, y las oportunidades que el mismo Manual presenta para reabrir debates en el tema del ciberespacio que parecían cerrados o que no parecían avanzar en cuanto a propuestas nuevas tanto a nivel particular (a partir de los participantes) como a nivel internacional.

- *Retos*

1. La noción sobre la Seguridad Nacional: Los acontecimientos cibernéticos ocurridos desde 2001 hasta el 2006 no habían sido primordiales para abrir debates sobre la seguridad del ciberespacio. No se habían logrado que se planteara una discusión fuerte sobre lo que se debería abordar al respecto. Tras los acontecimientos de 2007, Estonia se marcó como propósito convertirse en una potencia en ciberseguridad. Se replanteó los propósitos de su Seguridad Nacional y apresuró el debate dentro de la Unión Europea para renovar todas las directivas propuestas y mejorar los libros verdes sobre la protección de Infraestructuras Críticas.

Estonia se había convertido en el blanco fácil y en la prueba de que existían, aún, demasiadas debilidades en cuanto a legislaciones planteadas de manera nacional y a nivel Unión Europea. Se supone que para ese punto la Unión Europea ya tenía que estar en condiciones de afrontar problemas similares a los de Estonia, recién habían publicado su Libro Verde para la protección de Infraestructuras y llevaban políticas que tenían que proteger a sus miembros en el ciberespacio. Al final el miembro más desarrollado, tecnológicamente, y que representaba el prototipo de lo que la UE quiere llegar a ser como conjunto, terminó siendo desconectado por un ataque que pudo prevenirse.

Ni Estonia ni la UE son culpables de su ataque pero si hay que reconocer que muchas veces los debates de ciberseguridad planteados en la UE no eran lo suficientemente comprometidos con la ciberseguridad y tenían demasiados vacíos preventivos ante este tipo de ataques. En cuanto Estonia, el país era uno de los más desarrollados pero muchos de sus mecanismos de prevención

eran similares a los de la Unión Europea y esto provocó que no se encuentre preparado para manejar un ataque de tal magnitud.

Tras ocurrir los acontecimientos, Estonia comprende que la cuestión de Ciberseguridad Nacional tiene que ser más estricta y preventiva para no volver a ser un blanco fácil de ciberataques. En especial de un país con quien tiene choques políticos constantes. Y siendo el prototipo de lo que la UE quiere llegar a ser, es necesario el trabajo en conjunto para poder crear una política de seguridad viable y aplicable a toda la Comunidad europea.

El reto más evidente es el cambio a la noción de la Seguridad Nacional. Los ataques cibernéticos transforman los retos que cada país tiene con la Seguridad. Dependiendo de las características del país, sus fortalezas y sus debilidades. Los elementos que componen a la Seguridad se transforman y tiene que ser actualizada para prevenir cualquier ataque al país. Tras los nuevos enfrentamientos en nuevo espacios, la Seguridad se modifica y es necesario adaptarse a ello. Por eso el reto de la UE es claro, el trabajo de cada miembro por reforzar su Seguridad Nacional y a partir de ellos trabajar en conjunto. La UE puede funcionar hasta que las seguridades nacionales se fortalezcan y de cierta forma se acoplen para tener los mismos intereses presentes.

2. Actores activos en el enfrentamiento asimétrico: De esta cuestión ya se ahondó en los apartados anteriores. Es, quizá, el mayor reto del Manual y de cualquier legislación sobre el ciberespacio. La diferencia entre actores es enorme, en especial en un espacio donde el enfrentamiento puede ser contra cualquiera. El Manual y el Grupo de Expertos tiene que conocer, a gran escala, las capacidades de cada uno de los actores posibles y crear pautas que permitan orientar dentro de un conflicto de este tipo. Este es uno de los mayores retos porque se deben de establecer formas de ataque o patrones, que puedan diferenciar el ataque de un Estado al de un grupo hacktivista.

Una de las posibilidades sería las intenciones con las que se busca atacar a otro sujeto pero sigue siendo un poco variable el resultado de estas posibilidades. Es lo complejo de este punto, la intención, los actores que pertenecen y el origen de cualquier ataque. El Manual de Tallin proclama que se considerará cualquier tipo de ataque, pertenezca a quien pertenezca y en las condiciones que se haga (se esté en guerra o no), será como un acto de

guerra. Esta es una cuestión fundamental a tratar, pues es probable la violación de derechos humanos. A lo largo de la historia en que el Estado ha interferido en el ciberespacio, la sociedad civil es la que reacciona ante todas las imposiciones que se le plantean. La Declaración de Independencia del ciberespacio o la mitificación de los grupos de hackers como lo es Anonymus, han producido, en la sociedad una voz ante cualquier intento del Estado por censurarla.

Es por ello que, los actores que participan en esta dinámica representan uno de los principales retos del Manual. Manning o Assange, son personajes que en su momento descubrieron varios hechos contra varios gobiernos. Esto conllevó a sentencias en prisión para Manning quién fue condenada a 35 años de prisión en 2013 pero liberada[186] en 2017 por el perdón que le otorgó el presidente Obama. Este último ejemplo es importante destacar pues siendo el personaje que representó Manning y que violentó la seguridad de Estados Unidos, fue liberada tan pronto y terminó convirtiéndose en un tipo de héroe, da mucho qué pensar.

El daño que representó para los Estados Unidos fue importante pero con la prisión no se le podía castigar pues ya lo había cometido, más que un crimen sin víctimas es un crimen que ponía en juego la seguridad nacional estadounidense. Tras salir de prisión se engrandece su personaje y hasta es posible que haya sido liberada por la misma cuestión: la imagen de hacker héroe contra el gobierno. Aún así, el trato de prisionero de alto riesgo no elimina el hecho que los daños fueron en la red y aunque se le castigue con encarcelamiento o prohibición de acceso a la red, se debería de cuestionar qué tipo de sanciones serían las adecuadas para este tipo de situaciones.[187]

Y este es uno de los debates más importantes, tanto por el Manual en Europa como a nivel Internacional. El tipo de castigos aplicables y lo efectivo que serían tanto a favor de quien fue afectado. Es evidente que la información puede representar una debilidad para los Estados, la forma en que funciona la política, entre otros temas más graves. Al final, si el gobierno estadounidense buscaba un castigo, enviarlo a prisión no solucionó nada. Es el gran dilema. Si

[186] En un inicio era Bradley Manning pero cambio su sexo en 2014, tras ser condenado a 35 años en prisión.

[187] Actualmente se vigila en la red sus acciones y que no vuelvan a cometer crímenes de tal índole.

se encuentra al autor de un ataque cibernético, se enjuicia y se le dan años en prisión, no habrá una compensación justa a la hora del castigo. Y aunque sea considerado un enemigo de guerra, solo queda pensar que habrá castigos severos y eso puede ser perjudicial teniendo en cuenta que no se suelen respetar los Derechos Humanos en estas situaciones.

Este es reto es primordial para el debate tanto en el Manual como para la sociedad internacional. Entender el perfil de los atacantes y a partir de ahí saber cómo actuar es fundamental. El grupo de expertos solo ha transcrito la idea de la guerra al ciberespacio, en este aspecto, y no ha hecho un desarrollo a profundidad sobre todas la posibilidades dentro de todos los actores en un conflicto asimétrico en el ciberespacio.

3. Las responsabilidades del Estado: El Manual se crea para poder darle al Estado, y a los actores tradicionales, una mayor participación en el ciberespacio. Se le atribuye a los Estados responsabilidad pues serán ellos quienes evalúen el conflicto y determinen si es posible atribuirle a otro Estado la autoría del ataque. O crear legislaciones internas que les permitan solucionar el conflicto en cuestión. Pero es aquí cuando surge un problema, "muchas veces es el apoyo técnico el que tiene más desarrollo que el jurídico y es justamente esta cuestión una problemática para el Manual"[188]. Si el Manual de Tallin pretende ser una base jurídica para la resolución de estos conflictos, no está planteando bases tanto para determinar un culpable como las responsabilidades que el Estado tiene que tener al momento de medir los daños.

El Manual explica que cada Estado puede hacer lo que quiera en sus Infraestructuras pero si empieza a tener efecto en las de otro Estado será considerado como un ataque. Y también contará con soberanía estatal en donde nadie podrá intervenir en las IC cibernéticas. El reto será comprender cómo y cuándo una IC es violentada, la intrusión del enemigo e identificar actividades ilícitas dentro del territorio al que pertenecen. Las IC son la referencia pues es a partir de ellas que se puede identificar si se ha violentado a otro Estado y ese también es un margen de mucho riesgo que tampoco ha sido considerado en el Manual.

188 Vázquez Ortiz, Ana Pilar (2016), Op. Cit.

4. Infraestructuras Críticas compartidas: Las IC son un punto fundamental para toda la cuestión del ciberespacio. En el caso de las IC compartidas, no existe una concesión en el Manual que explique las medidas a tomar en estos casos. Por ejemplo, la Unión Europea cuenta con este tipo de IC o los países, comúnmente en sus fronteras. El Manual no explica cómo debe desarrollarse la resolución del conflicto, los acuerdos a los que hay que llegar para implementar un castigo, en especial cuando las legislaciones nacionales son totalmente diferentes o tienen una política de seguridad enfocada a diferentes cuestiones.

El reto de este punto será crear un consenso entre las partes afectadas que se adapte a las necesidades de cada una, de sus legislaciones nacionales y que sea aceptada, y acatada por todas las partes. El Manual debe enfocarse en los criterios que se irán resolviendo como el considerar al más afectado, el punto débil entre los afectados[189], las cuestiones a tratar, las prioridades, los mecanismos en que se buscará localizar al autor de los ataques y las posibles sanciones si pertenece a otro Estado.

5. El enfoque del Manual: Una de las debilidades del Manual es que se centra en tecnicismos legales en vez de la cuestión informática que puedan agregar más variedad y más contenido a los debates sobre la legislación del ciberespacio. La técnica es más avanzada que la legislación, pero es justamente un trabajo en conjunto lo que lograría que el derecho se vuelva más dinámico y acorde a la velocidad con se quiere rectificar el manual de Tallin.

Aunque el Manual cuenta con expertos en estos temas y que han trabajado en cuestiones similares, es evidente que no se enfocan en el contenido del ciberespacio. Como se vio en el capítulo 1, la composición del ciberespacio es muy amplia, la cibergeografía contribuye a que se comprenda más el mismo ciberespacio desde el interior y esto debe ser parte del debate del Grupo de Expertos porque ampliaría la visión en muchas cuestiones a tratar y no solo enfocarse a trasladar los tratados y manuales de la guerra física a la guerra cibernética.

[189] Si se entró a partir de las redes de un país que no tiene una política de prevención ante este tipo de eventos o la debilidad de una IC de alguno de los afectados en un ciberataque.

6. El compromiso sobre la doctrina: Si se le pregunta a cualquiera de los participantes en los debates del Manual sobre si es una doctrina que se tomará a futuro o se considerará como algo viable a rectificar, recalcarán constantemente que no tienen ningún compromiso con el Manual. Es solo un debate entre expertos que no compromete a los miembros que representan. Y esto es entendible pues el Manual ha mostrado muchas debilidades en su desarrollo, tanto en la primera versión como en la versión 2.0 (publicada en 2017) existen muchas carencias que ningún actor está dispuesto a soportar. Son, quizá, estas carencias lo que no permiten que se acepte como una posibilidad legal.

La otra cuestión es el aceptar que al final el Estado y los organismos internacionales tendrán el control del ciberespacio. Esto provocaría muchas discordias entre todos los participantes pues el que un solo actor pueda tener el control iría contra los intereses de todos. Y no es que un Estado gobierne el ciberespacio ahora sino que buscará imponer sus reglas a conveniencia lo cual frenaría el desarrollo de muchas acciones dentro del ciberespacio. Este último punto es el que siempre importa pues es el que terminará afectando las relaciones con otros actores en el ciberespacio.

En un supuesto de que se aceptaran las normas del Manual de Tallin y se buscará una legislación internacional en donde el Estado es el que controle, en mayor medida, la dinámica del ciberespacio, muchos actores participantes no estarían de acuerdo con ello. En un mundo globalizado, el que un actor sea el “justiciero” de un espacio que ha sido libre (no ha existido nada que limite su desarrollo) desde su creación no será aceptado tan fácilmente. En especial si hablamos de un actor tan centralizado como lo es el Estado. El legislar el ciberespacio, a partir de un actor clásico, significaría demasiadas desventajas que nadie quiere tener.

No son solo los intereses económicos, como el que podrían representar las empresas, sino son actores de todo tipo que tienen un papel activo en el ciberespacio y una legislación fuerte dentro de él los limitaría. Por ejemplo, universidades o instituciones de investigación podrían perder las oportunidades de investigación, habría reglas demasiado estrictas que vayan contra estas mismas instituciones y las investigaciones no avanzarían a un ritmo acostumbrado. Otro ejemplo serían los hacktivistas, al gobernarse el

ciberespacio (por decirlo de algún modo) por el Estado, el control de actividades de este tipo sería más estricto y sus acciones, si van contra lo impuesto, podrían considerarse como acciones de guerra.

El Manual y lo establecido es un arma de doble filo. Por eso ninguno de los participantes lo ha adoptado como doctrina, existen diferentes contradicciones e intereses que chocan, además de que se adjudicarían responsabilidades que aún nadie está dispuesto a enfrentar. Tendría que ser un actor influyente de manera global para que se lograse un cambio. El que ya la OTAN se esté encargando de este debate es importante, no es una doctrina aceptada pero ya es una posición ante el mundo y las preocupaciones que se tienen con respecto al ciberespacio.

Rusia, constantemente, ha buscado una forma de que el ciberespacio sea regulado por Naciones Unidas, justo después de que se enterara de la intención de crear este Manual. Aunque la OTAN no ha señalado como algo factible de aplicar si lo posiciona en un interés de no compartir el control del ciberespacio más que con los socios más cercanos a Estados Unidos. Es una lucha por el dominio de otro espacio. Y este será el mayor reto a tratar pues mientras ninguno se proclame con un instrumento jurídico aplicable que comience a regular los ciberataques ninguno se proclamará con una doctrina a seguir y las cuestiones del ciberespacio seguirán el rumbo que tienen actualmente.

- *Campos de acción*

1. Nuevos enfoques de estudio: Como se menciona en el reto 5, el enfoque fuera de lo legal sería un buen inicio para considerar estudios del ciberespacio como la cibergeografía para poder comprender al ciberespacio como un espacio más real. Además de otros estudios alrededor del ciberespacio que puedan ampliar el debate del Manual y que permita una continua retroalimentación desde diferentes aristas. Y de esa forma no solo tener un enfoque a partir de lo ya experimentado (con los convenios y manuales de guerra física) sino crear escenarios futuros factibles sobre el ciberespacio.

2. Renovación de las características que conforman el concepto de Seguridad Nacional como algo prioritario: Es evidente que el ciberespacio ya es una prioridad en la agenda internacional pero a su vez no tienen un enfoque amplio para poder catalogarlo como una amenaza latente en muchos aspectos. Es por ello, que con todos los debates del Grupo de Expertos, se pone a juicio si los Estados realmente han tomado este tema como uno necesario en la agenda nacional y en sus políticas nacionales de seguridad. Es a partir de aquí que se abre la puerta a que cada país analice la prioridad de renovar su percepción de Seguridad Nacional en un mundo tan cambiante y en un espacio del cual dependemos cada vez más.

3. Legalidad del ciberespacio y acuerdos internacionales posibles: Este punto es lo más destacable que ha traído el Manual. Es a partir de su creación que países, como Rusia, planteen un instrumento jurídico aplicable al ciberespacio en donde todos tengan una participación y que sean los gobiernos los que restrinjan las actividades del ciberespacio. Pero es evidente que acciones como las de Rusia no funcionaran debido a que una aceptación violentaría muchas libertades individuales.

El foro de la Secretaria de Seguridad de Nacionales Unidas, Foro sobre la gobernanza de Internet, son un intento por crear acuerdos internacionales que permitan el manejo seguro de internet y del ciberespacio en general. Lamentablemente estos foros no han tenido el impacto necesario para que se cree un interés, a nivel internacional, sobre un convenio sobre la legalidad del ciberespacio. El Manual vuelve a presentar una oportunidad para que se plantee un acuerdo internacional con el mismo propósito.

4. Cooperación respecto a la ciberseguridad (regional e internacional): Respecto a punto anterior, el crear acuerdos y convenios facilitaría la cooperación entre diferentes países para crear mecanismos de ciberseguridad. Estos podrían presentarse a nivel regional, nivel continental o nivel internacional que faciliten la cooperación de los países en el ámbito de la ciberseguridad.

Tras el análisis a los temas más importantes del Manual de Tallin, aún existen vacios en el debate sobre lo que debería o no aplicarse al Manual. Además de la aceptación que debe recibir a nivel internacional. Si se convertirá en un Manual más sobre la legalidad en Internet o será la base para

propuestas mejor trabajadas tanto a nivel Unión Europea como a nivel internacional que realmente trabaje la cuestión del ciberespacio.

3.4 El tiempo de Estonia: las propuestas como presidente del Consejo Europeo

> *En Europa, la fuerza de la ley sustituyó a la ley del más fuerte (…) En la Unión Europea, el Estado de Derecho no es una opción. Es un imperativo. El Brexit no definirá esta presidencia, porque se trata de una negociación. Y nosotros vamos a ayudar para que la negociación sea rápida, y confío en que Reino Unido respete los derechos humanos en todo este proceso, porque es una democracia.*
>
> *Presidenta de Estonia, Kersti Kaljulaid*

El segundo semestre de 2017, Estonia se posiciona como el presidente del Consejo Europeo con el plan de hacer Europa Digital. Las experiencias tenidas en 2007 le enseñaron sus debilidades y ahora que ha trabajado en fortalecerse, quiere que la misma Unión Europea siga sus pasos. Ya sea por posicionarse, en la UE, como un miembro influyente en la toma de decisiones sobre lo digital; o por encontrar una mejor unión en sus relaciones exteriores con el resto de los miembros de la Unión, y así logrando disminuir aún más sus relaciones con Rusia, el objetivo de Estonia es comenzar medidas fuertes que apoyen los objetivos 2020.

Tras la renuncia de Reino Unido a la presidencia debido al caos de Brexit, Estonia toma su lugar y comienza a desarrollar su plan para fortalecer a la Unión Europea y lograr la digitalización, que es un plan ya abordado desde bastantes años atrás. Tras la renuncia de Reino Unido a asumir la presidencia del Consejo Europeo, Estonia, e inmediato, presentó un planteamiento de 5 puntos significativos sobre sus objetivos a lograr en su presidencia y las negociaciones con los miembros de la Unión y socios más importantes.

- Reforzar la Agenda Comercial Europea

El comercio es un punto importante para la UE. La apertura comercial en la Unión Europea la ha convertido en un atractivo comercial para todo el mundo.

El propósito de Estonia es que estos acuerdos se efectúen antes de finalizar su mandato.

- Una Industria más fuerte y competitiva

Se enfoca en la industria automovilística. “La nueva Estrategia de Política Industrial que presentamos hoy ayudará a nuestra industria a mantener una situación puntera en innovación, digitalización y descarbonización”.[190]

- Lucha contra el cambio climático

Tras el abandono de Estados Unidos del Acuerdo de París para la protección del medio ambiente, la Unión Europea buscará posicionarse como el que encabece este acuerdo para que no se pierdan los logros ya obtenidos.

- Los Europeos y la era digital

Se desea continuar con el mantenimiento de la seguridad en línea. Se plantearán nuevas normas y propuestas y se continuará con el reforzamiento de la lucha contra la propaganda terrorista y la radicalización de internet.

- La inmigración en Europa

Pese a la gran controversia del tema, se han conseguido progresos importantes. Se busca mejorar la protección a las fronteras exteriores de Europa. Con el fin de reducir el número de muertos en el Mediterráneo, se pretende reforzar las fronteras. El Alto Comisionado de Naciones Unidas para los Refugiados (ACNUR), presentó una serie de propuestas para Estonia donde se trabaje con mayor responsabilidad la cuestión de los refugiados.

Bajo una presidencia bastante caótica, Estonia se mostró optimista pero siempre concentrado en una cuestión: la digitalización de la Unión Europea. Si bien, había cuestiones de índole más urgente, Estonia se enfocaría en que la parte comercial de la UE no se viese afectada. Su planteamiento para lograr esta digitalización se concentrará en la descentralización de datos y en el mejoramiento de la seguridad digital. Esta descentralización de datos es una alternativa que permitirá compartir información a diferentes puntos del mundo cuando un Estado esté siendo atacado. La base que actualmente plantea Estonia podría ser un inicio a la Política conjunta de Seguridad y Defensa.

[190] *Ídem*

3.4.1 Embajadas Digitales y la protección de Datos

Las embajadas digitales han surgido como una forma de descentralizar la información de un Estado y de todas sus funciones. Una de las lecciones más importantes que les dejó el enfrentamiento en 2007 es que si se vuelve a atacar al Estado completo y se paraliza puede ocurrir una tragedia: la pérdida de toda su información. Estonia es el gobierno sin papel de la Unión Europea, el 98% de sus transacciones son digitales y la pérdida de ellas podría ser un problema enorme si solo en el país se mantiene esa información.

Para este momento existirán dos tipos de embajadas digitales presentadas por la UE. Una es por Estonia y la otra por Dinamarca[191]. La de Dinamarca consiste en hacer buenas relaciones con las principales empresas, de cada país, y abrir una embajada similar a la física pero que sea en cuestiones de ciberespacio. El plan de Dinamarca sobre esta embajada digital es trabajar con Silicon Valley para crear buenas relaciones comerciales que a la larga sean beneficiosas para el país. Al igual que con una embajada política, la embajada digital responderá a los intereses en el ciberespacio y en especial con las empresas que trabajan en internet. Así ampliar el mercado digital y lograr buenas relaciones si en un futuro son necesarias.

La presentada por Estonia, como se explica al inicio, es para descentralizar. Es crear otra embajada donde se puedan instalar todos los datos del país. Es como si se recreara Estonia en otros países pero solo a partir de lo digital. La primera de este tipo fue creada en Luxemburgo[192] debido a las buenas relaciones que se tienen con ese país. Se busca que este tipo de embajadas se implementen en toda la Unión Europea y con todos los Estados Miembros. Pero primero se tiene que saber si es una opción que realmente dé resultados, por ello esta primera embajada podría representar un gran cambio a la forma de protección de datos donde no solo es a un actor en un solo sitio sino a un actor que está distribuido en diferentes partes.

A partir de esta idea, junto con Microsoft, se busca crear un sistema, similar a la nube de Google, que le permita a Estonia tener todo el control de

[191] Domínguez Cebrian, Belén (28 de Marzo de 2017), Dinamarca abre embajada en Silicon Valley, *El País*, Madrid, España. Recuperado de: https://goo.gl/A4HBuL

[192] Navarro, Beatriz (4 de Julio de 2017), Estonia abre la primera embajada digital para proteger sus datos, *El país,* Tallin, Estonia. Recuperado de: https://goo.gl/LZZhBT

sus datos sin necesidad de que terceros participen en ello y así asegurar sus datos. La idea de esta nueva embajada es tener un tercer refuerzo si se llegase a perder la información de un país o las embajadas que tiene el país en todo el mundo por un ataque cibernético.

Estas embajadas buscan ser protegidas a partir de lo acordado en la Convención de Viena sobre las embajadas tradicionales y trae a la mesa un nuevo tema de debate sobre el uso de estas embajadas, sus funciones y lo que pueden implicar en el ciberespacio. Pues, a diferencia de sus análogas físicas, las digitales se concentran en lo que se encuentra en el ciberespacio y en el ciberespacio es difícil recrear fronteras.

La liberación de datos permitirá que se logren las medidas de la Unión Europea planteadas en la Estrategia Europa 2020. Se eliminan "normas de acceso y portabilidad de datos, se eliminan los requerimientos de geolocalización y el compartir datos entre las diferentes administraciones sin trabas"[193] para poder lograr esa Europa Digital 2020.

La presidencia de Estonia en el Consejo Europeo[194] fue el inicio del planteamiento de muchos temas, en especial en el campo digital. La integración fue la base para que se pusieran a debate y que fueran un objetivo a alcanzar en el futuro. Aún así, quedan los problemas que vienen acarreándose desde hace mucho tiempo en la UE. La debilidad en la integración europea, el Brexit y Cataluña han puesto en jaque los propósitos de unificar toda Europa y de hecho han demostrado que los intereses de cada miembro son tan diferentes, y a veces van contra la misma integración, que el debate de lo que le espera a la Unión Europea se amplía a aquellos objetivos ya logrados.

Hay que agregar las problemáticas que el gobierno de Donald Trump han traído para la Unión Europea, y no tener ya tanta confianza en los mecanismos de seguridad que los unen con Estados Unidos, ha comenzado un cuestionamiento por los miembros más influyentes.

Siendo la OTAN la alianza más significativa para la Unión Europea, se debe de reconsiderar para entender todas las propuestas del Manual de Tallin

[193] Coello, Claudio (2017), La Europa Digital: competitividad, progreso e integración, *Comisión Europea*. Recuperado de: https://goo.gl/WMqyRm

[194] EU2017.EE, Speech by Estonian Prime Minister Jüri Ratas: a review of the Estonian Presidency, *EU2017*. Recuperado de: https://goo.gl/YTgDCi

y las decisiones propias dentro de la UE. Esta relación es su conexión directa con Estados Unidos como socio y es la misma que ha representado problemas para acuerdos entre los miembros de la Unión Europea y debilita más su integración. Se debe repensar, a partir de los problemas de su relación, las posibles acciones a futuro de la Comunidad europea.

3.4.2 La OTAN y la Unión Europea

La relación de la OTAN con la Unión Europea parte desde los intereses comunes de ambos y que responde al intento de defensa de un período de la historia. Sin embargo, en la actualidad esa relación de verdadera cooperación se ha visto quebrantada ante los intereses de los diferentes actores. Los choques políticos, en su mayoría, han provocado choques de intereses entre los miembros de la OTAN. Además, debido a que no todos los miembros de la Unión Europea pertenecen a la OTAN, quienes no pertenecen se han visto bastante cerrados y en contra a las acciones efectuadas por el organismo.

Si duda alguna, estos enfrentamientos han provocado la desunión de la Comunidad europea, además de que la mayoría de las decisiones en la OTAN han ido en pro de Estados Unidos, en muchos casos, sin tomar en cuenta la decisión del resto de los miembros[195]. Ahora hay más desunión en la OTAN que en otros años. El poco liderazgo y las malas decisiones de Trump han provocado que los miembros la Unión Europea que pertenecen al organismo ya no quieran ser parte de esta alianza. Ahora la Unión busca unificar más a sus miembros y a partir de ello crear mecanismos de seguridad óptimos que aseguren sus propios intereses.

Tras el anuncio de sus intenciones sobre crear su propio ejército, Estados Unidos estuvo totalmente en desacuerdo con las intenciones europeas. Este ha sido uno de los problemas principales, los desacuerdos constantes respecto a los intereses estadounidenses y los propios como conjunto. “Conceptos como multilateralismo y acción preventiva adquieren distintas interpretaciones que afectan a la cooperación práctica entre los EEUU

[195] Como el hecho de que no todos los miembros europeos de la OTAN estaban a favor de la guerra de Irák.

y algunos de sus aliados europeos".[196] Esta unión, en un momento fue eficaz y funcionó para su propósito pero debido a los diferentes intereses y las desestabilidades de sus miembros (principalmente la misma UE), ya no trabaja de la misma manera.

Recientemente la Unión Europea ha promovido un sistema de defensa propio tras la inestabilidad de Estados Unidos para liderar. Como era de esperarse, Estados Unidos se ha opuesto a esta propuesta debido a que implicaría un descontento en sus relaciones. Si bien ya existen mecanismos de defensa conjunta como el NRF (NATO Response Force) o los Battlegroups.[197] Estos mecanismos han funcionado para que la Unión Europea equilibre sus intereses militares con Estados Unidos sin que interfiera con la Alianza Atlántica. Aún así, su relación ha demostrado cierta inestabilidad en los últimos años.

Hay que destacar un punto importante, pese a que la Alianza se crea con ciertos fines en la Guerra Fría, tras la caída del Muro de Berlín, los europeos han buscado retomar su propia defesa, en especial Reino Unido quien ha bloqueado la autonomía europea para darle cierta fuerza a la Alianza y a su vez esta se enfoque en la defensa europea. Tras el Brexit, esto cambia y le permite a la Unión Europea poder decidir, y replantear su seguridad en conjunto. Pero el principal problema seguirán siendo los intereses de los miembros de la UE.

Ha sido un choque de intereses bastante notorio, desde la desintegración del bloque soviético, los cambios de paradigma, las nuevas amenazas mundiales, la integración de países ex-soviéticos, el choque de intereses entre los miembros de la Unión Europea (pertenecientes y no pertenecientes), el uso de la OTAN como elemento meramente simbólico para los intereses estadounidenses, entre diferentes aspectos, son todos los elementos que han provocado la desestabilidad de la Alianza y de la Unión.

> A finales del año 2011 y principios de 2012 la administración Obama ya anunciaba claramente que quería incrementar el papel de

[196] Laborie Iglesias, Mario A. (2010); La cooperación OTAN-UE en el futuro concepto estratégico de la Alianza Atlántica*; Real Instituto Elcano*; Recuperado de: https://goo.gl/qGvNGu

[197] Estos son europeos pero su funcionamiento se enfoca a ser un apoyo a la OTAN donde el más beneficiado sea la Unión Europea y no Estados Unidos. Es una forma de equilibrar las posibilidades con Estados Unidos.

> Estados Unidos en la región Asia-Pacífico, tanto en los ámbitos de su política económica, política exterior y en su política de seguridad. El cambio en las prioridades estratégicas de los Estados Unidos levantó rápidamente todos los temores en el seno de los países europeos, acostumbrados a que los Estados Unidos les sacaran las castañas del fuego. Los 100.000 efectivos que Estados Unidos tenía desplegados en Europa en 2005 seguían reduciéndose, llegando a unos 62.000 en 2016. El "desenganche" de Estados Unidos de la seguridad del Viejo Continente ya no era sólo una amenaza, sino que se estaba produciendo en la realidad. Pero no se estaba llevando a cabo porque los propios países europeos fueran capaces de asumir un mayor peso en su propia defensa y la participación norteamericana fuera menos necesaria, como algunos países llevaban décadas soñando. Se producía porque Estados Unidos identificaba sus principales intereses en otra región, y consideraba que Europa debía poder encargarse de los asuntos que principalmente les afectaban a ellos, en unos tiempos en los que la escasez de recursos era un problema importante para todos.[198]

Este es un tema también importante para la relación con la OTAN. El gasto económico entre los miembros ha sido dispar. Pocos de los países pertenecientes a la Alianza han aportado el 2% del Producto Nacional Bruto a la defensa. Estados Unidos ha llegado a aportar el 5.29% del PNB. Esto es, en parte, por lo que Estados Unidos ha decidido enfocarse en otras cuestiones, reducir el gasto pues la mayor parte de él ha sido para Europa. La guerra de Libia de 2011 fue donde las intenciones de Estados Unidos fueron claras, pues la armonía entre los europeos ni existía. Tras el voto de la intervención militar en el Consejo de Seguridad de Naciones Unidas, los europeos se mostraron bastante dispares en sus decisiones.

La diferencia de intereses fue visible y Estados Unidos decidió dejarles el cargo de toda la operación a los europeos. Reino Unido y Francia fueron los que hicieron el mayor esfuerzo. El resto solo apoyo de manera secundaria. Esto es importante retomar porque plantearía las posibilidades, a futuro, si la Unión Europea realmente está interesada en crear una estrategia de seguridad y sus miembros están dispuestos a aceptar esto y participar de forma activa. A partir del alejamiento de Estados Unidos de la Alianza, las debilidades en la unificación de la Comunidad europea son evidentes y solo será la Comunidad europea que lo haga posible.

[198] García, Javier (2016); La Unión Europea y la OTAN en el marco de la Nueva Estrategia Global de la Unión Europea*; UNISCI*,(No. 42), p. 16

Sin Reino Unido que límite la seguridad conjunta, pues aunque no pertenece de facto a la UE si suele tener gran influencia en esta, se puede promover de mejor manera la cooperación conjunta en temas de defensa sin tantos enfrentamientos de opinión. Una seguridad conjunta en la que todos los miembros estén de acuerdo. Las posibilidades de crear una Política Común de Seguridad y Defensa debe aumentar el compromiso de los miembros. La OTAN comenzaría a ser la parte débil de la alianza con Estados Unidos y Reino Unido, si se sale de la Unión, sería el que menos poder tendría en las decisiones conjuntas europeas.

Esta nueva integración tendría diferentes beneficios:

- Mayor integración en la política exterior de los miembros al crear objetivos comunes.
- Mayor refuerzo en organismos como la ONU o la OTAN a partir de los intereses europeos.
- Ampliar capacidades de colaboración con la OTAN (se quiera o no, Estados Unidos seguirá siendo un socio importante para la UE).
- Se adaptaría una estrategia para Europa y los intereses que le competen solo a este continente.

Pero la salida de Reino Unido de la UE no traerá, en su totalidad, beneficios a la Unión. De ahí que aún se luche porque este país no salga. Para el otoño de 2018 se resuelve la cuestión y si Reino Unido sale, la Unión Europea tendría muchos asuntos por resolver sola pues Reino Unido es un miembro importante y bastante activo en la cuestiones de Unión Europea. Si bien, en muchos aspectos podría verse beneficiada la Comunidad europea, no sería hasta la salida de Reino Unido que tendremos las consecuencia de ello y esto no ayudaría a la estabilidad de intereses de los miembros, además que alentaría la salida de algunos otros. Esta decisión podría representar una transformación profunda para la Unión Europea, en especial cuando su unión ha sido tan cuestionada y suele estar siempre en la cuerda floja.

3.5 Planteamientos de una política de ciberseguridad y defensa conjunta

> *La Unión Europea tiene que estar dispuesta a asumir su responsabilidad en el mantenimiento de la seguridad mundial y la construcción de un mundo mejor, o su determinación a actuar desde el primer momento, […] debemos estar preparados para actuar antes de que se produzca una crisis. Nunca es demasiado pronto para prevenir los conflictos y las amenazas.*
>
> *Estrategia de Seguridad Europea 2003*

Antes de abordar la cuestión de ciberseguridad, es necesario hablar de los planes en seguridad y defensa de la Unión Europea. En la cumbre de Bratislava de 2016, la UE impulsó la idea de la seguridad exterior y defensa europea a partir de la cooperación entre los Estados miembros. A diferencia de los planes que tienen otros países de adoptar medidas solo para Europa, se establece, en la cumbre, un plan de cooperación más fuerte con la OTAN. Aunque dejó a discusión el desarrollo de la política de seguridad y defensa de la UE.

Más adelante, la Estrategia Global de la Unión Europea, plantea una aplicación centrada en tres prioridades: "dar respuesta a conflictos y las crisis exteriores; aumentar las capacidades de los socios; y proteger a la UE y sus ciudadanos".[199] Además de ampliar estas capacidad e instrumentaciones militares a otros campos como es el ciberespacio. Se han plasmado varias ventajas si se logra aumentar la transparencia y visibilidad política de la defensa europea:

- la mejora de la detección de carencias
- la intensificación de la cooperación en materia de defensa
- un planteamiento más adecuado y coherente de la planificación del gasto en defensa

A mediados de junio de 2017, la UE pretende buscar la cooperación estructurada permanente para asegurar y reforzar la seguridad y defensa de

[199] Consejo Europeo (2016), Cooperación de la UE en materia de seguridad y defensa, *Consejo Europeo,* Recuperado de: https://goo.gl/Bj8nNR

Europa. Hasta ahora solo han sido 25, de los 28 Estados miembros lo que han apoyado las iniciativas de cooperación para seguridad y defensa. Se han aprobado varios proyectos que puedan fortalecer esta cooperación: formación, desarrollo de capacidades, disponibilidad operativa, entre otros.

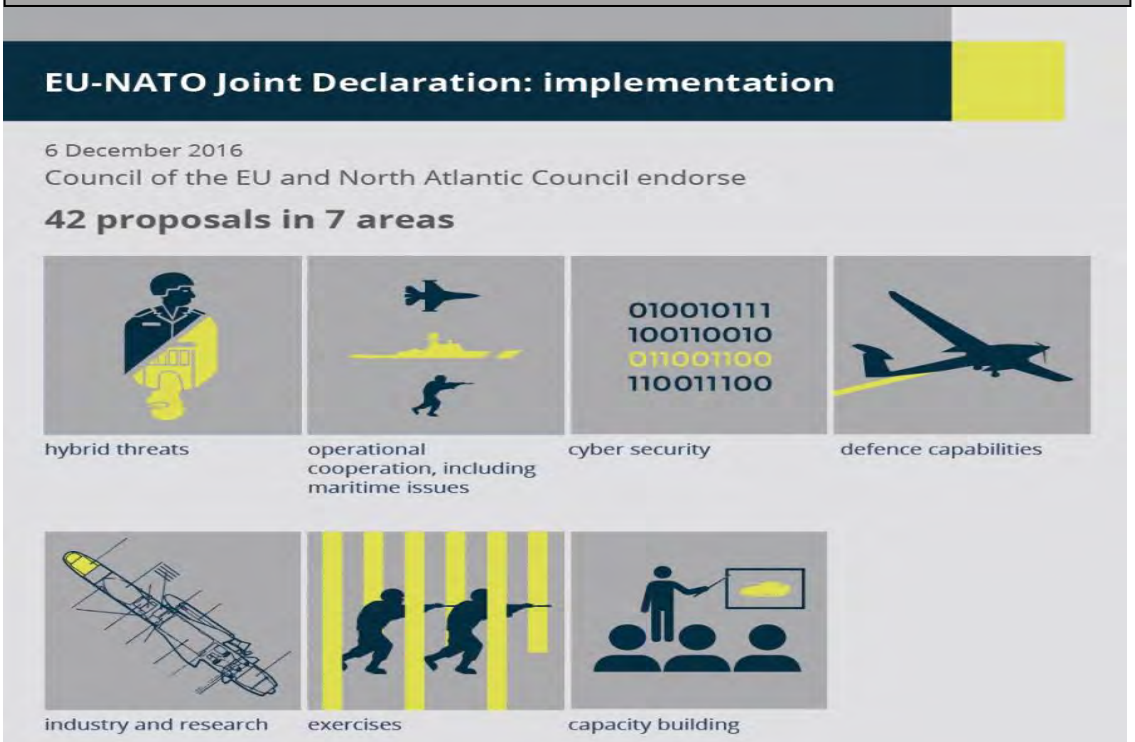
Esto con la posibilidad de mejorar la capacidad de respuesta ante una crisis de manera eficaz, rápida y coherente. Es a partir del despliegue de Battlegroups (propuesto en 2007) que se ha planeado lograr esta eficacia pero es hasta junio de 2017 que ha planificado la financiación de los mismos. La prioridad ahora es la cooperación con la OTAN pues antes de conseguir una defensa propia, se tiene que mantener en buenas formas la alianza de seguridad. En julio de 2016, OTAN y la UE hacen una declaración conjunto que señala 7 ámbitos estratégicos (como se muestra en la **imagen 10**): [200]

1. Amenazas híbridas
2. Cooperación operativa
3. Ciberseguridad
4. Capacidades de defensa
5. Industria e investigación
6. Maniobras coordinadas
7. Refuerzo de las capacidades

Es esta relación con la OTAN lo que definiría, y definió, las decisiones sobre la seguridad de la Unión Europea. Tras todo el análisis sobre la relación con la Alianza, se puede confirmar que aún es una relación importante para la Unión Europea pero a su vez la ha detenido para consolidar su propia seguridad. Es a partir de todos los cambios que está sufriendo la Unión que debe de considerarse, en mayor medida, el compromiso de sus miembros por asumir una doctrina de defensa conjunta. Y aunque debe partir de los intereses de cada miembro, la clave será el tener una verdadera intención de no depender de terceros para la seguridad de la UE.

[200] *Ídem*

Imagen 9. Propuesta de la OTAN para la construcción de su Política de Seguridad y Defensa en conjunto a la Unión Europea.



Estas medidas surgen a partir del Manual de Tallin pues se busca dejar en claro los propósitos de la OTAN con respecto a tomar posicionamientos e diferentes aspecto, como lo es la ciberseguridad. Es para esclarecer que es una doctrina que aún no es oficial.
Fuente: Consejo Europeo (2016), Cooperación de la UE en materia de seguridad y defensa. *Consejo Europeo.* Recuperado de: https://goo.gl/Bj8nNR

En el ámbito de la ciberseguridad, en la relación de la OTAN y la UE, así como la UE por su cuenta, es un punto fundamental a tratar. Ambos trabajan bajo una línea similar las cuestiones del ciberepacio y su política al respecto. No es muy alejada la idea de que las discusiones en el Manual de Tallin puedan ser retomadas para los interese de la UE. Y este es el punto principal a tratar. Lo viable del Manual de Tallin que sea aplicable a los intereses europeos y en sí mismos sean una influencia para el resto de la sociedad internacional.

La propuesta es tomar las ideas más sobresalientes del Manual de Tallin, juntar a los expertos en el tema pertenecientes a cada miembro de la UE, y que a partir de los intereses de cada miembro se discuta la viabilidad de estas ideas para toda la Comunidad Europea, sean consideradas aplicables para una doctrina de ciberseguridad europea y se implementen a la UE dentro de su política de seguridad y defensa. Ya sea una sola para el ciberespacio o una donde el ciberespacio también esté incluido de forma prioritaria.

Algunos de los planteamientos a considerar son:

- Replanteamiento de las definiciones del Manual en aspectos como los ciberataques y comprender los grados de daño que lo considerarían un ciberataque. Muchas de las dudas que quedaba en el Manual era la composición de un ciberataque y hasta que nivel de daños puede considerarse como tal. A partir de las experiencias vividas por la UE, se tienen más elementos que pueden agregarse a la discusión.
- Retomar la importancia de las Infraestructuras Bilaterales o multilaterales, no dejarlo como una responsabilidad única del Estado al que pertenecen pues en el nuevo escenario global, todo está interconectados y las IC de la UE son parte de ello. Funcionan para todos los miembros y debe ser parte del interés de cada uno. Eso quitaría un poco de la soberanía nacional, pero si el propósito de la UE es la integración total, sería un paso más a ello.
- Repensar el Derecho Humanitario Internacional. Debido a que uno de los intereses principales de la UE es respetar, en mayor medida, los Derechos Humanos, podrían ser ellos quienes den un enfoque distinto aunque el Manual de Tallin presenta ciertas reglas que concuerden con este aspecto.
- Transformar la responsabilidad del Estado por una responsabilidad conjunta. Es evidente que el Manual de Tallin funciona para que un Estado pueda tomar medidas preventivas ante un ciberataque. Siendo la UE, tiene que existir un debate en conjunto sobre las medidas legales a tomar y que todos los miembros de la Unión estén de acuerdo. Además, esto presionaría aún más para que se haga una integración europea que permita que la responsabilidad de una IC pase a manos de todos los miembros en conjunto.
- Replanteamiento de las políticas de seguridad y defensa para plasmar los verdaderos intereses de la UE. Cada país miembro cuenta con una Estrategia de seguridad y defensa, cada miembro tiene una concepción del ciberespacio y por ende no existe una armonía sobre las cuestiones

primordiales a tratar en conjunto. Con un replanteamiento en las políticas de seguridad y defensa nacionales, que no se alejen de sus intereses pero que le den más importancia a los asuntos de la Unión y que exista más compromiso para su cumplimiento.

- Considerar que el ciberespacio tiene mayores efectos en la comunidad europea y a partir de sus intereses de integración digital, instaurar políticas que se apeguen a la defensa de sus redes. Además de una capacitación constante sobre los temas de ciberseguridad y de ejercicios en el ciberespacio que tengan un verdadero impulso en estas mismas políticas a nivel comunidad.

La idea de estos planteamientos es que la UE tenga una posición en su política de seguridad y defensa en el ciberespacio y no siga navegando en incertidumbre con políticas que tienen poco impacto para la resolución de estos conflictos. En especial, en los tiempos que el ciberespacio ha retomado una mayor fuerza y tiene más incidencia en el mundo físico. Agregando el interés de la Unión Europea por digitalizar su espacio, sus redes y crear una comunidad sin fronteras con el Mercado Único Digital que facilite el acceso de los ciudadanos europeos, su capacidad comercial y que tenga un impacto positivo en la integración conjunta.

Aún quedan muchos baches en el camino. De igual modo, la aplicación de normas de ciberseguridad a escala Unión Europea el pasado 27 de mayo de 2017, ya han demostrado las necesidades de la Unión. Entre sus intereses ya se ha plasmado la seguridad de redes de información, normas estrictas a operadores de servicio[201]y marcos nacionales y a escala de la UE para luchar contra las amenazas cibernéticas. Estas normas aún no están dentro de la aplicación legislativa pero el debate ya comienza a plasmar las necesidades. El Manual no será fácilmente aceptado como doctrina pero si traerá a la mesa elementos importantes no considerados en muchas políticas, en especial en la UE. El Manual de Tallin es un primer paso para la construcción de una verdadera política de Seguridad y Defensa en el ciberespacio para la Unión Europea.

[201] Este debe ser un tema que también debe retomar el Manual de Tallin porque son clave para los ciberataques. Y no se hace una alusión al respecto en el Manual que considero necesaria.

Consideraciones Finales

> *El problema no es de Internet. El problema es del sistema político. La sociedad modela a Internet, y no al contrario. Allí donde hay una movilización social, Internet se convierte en un instrumento dinámico de cambio social; allí donde hay burocratización política y política estrictamente mediática de representación ciudadana, Internet es simplemente un tablón de anuncios. Hay que cambiar la política para cambiar Internet y, entonces, el uso político de Internet puede revertir en un cambio de la política en sí misma.*
>
> Manuel Castells

El ciberespacio se convirtió en la revolución en el nuevo milenio y la globalización. Pese a ser un medio artificial (creado por el hombre) ha demostrado tener vida propia en el que cada vez más las personas estamos inmersas. Esto ha creado un cambio en la concepción de las relaciones sociales en donde el medio, internet, se convierte en el lazo trasfronterizo, algo que la globalización ha llegado a implementar. El mundo exige ser más global y el ciberespacio, junto internet, han permitido el desarrollo de esto.

Todo se conecta, cualquier situación puede conocerse en cualquier parte del mundo y tendrá efecto en el mismo. De igual manera, un nuevo medio se agrega a la dinámica del mundo que ha sido aprovechado, de nuevo por la mano del hombre. La economía mundial ya no solo se limita al espacio físico sino también al ciberespacio y este ha ayudado, en gran medida, a constituir el sistema capitalista en el que estamos inmersos. El ciberespacio se ha infiltrado en la humanidad y en sus estructuras básicas.

Esto ha permitido que se involucren diferentes tipos de actores en la dinámica del ciberespacio. Ya no solo son los Estados, los organismos internacionales, las empresas, las universidades, institutos de investigación, personas civiles con diferentes tipos de objetivos. Comienza una especie de anarquía, un nuevo medio que parece crear sus propias reglas aunque realmente son sus usuarios, sus actores, los que están moviendo los mecanismos de este nuevo sistema.

El ciberespacio supone la aparición de nuevos actores no estatales que han incrementando su capacidad para intervenir en todos los ámbitos. Con ello, implica mezclar todos los que competen a la actividad humana. Esto se convierte en un reto para la seguridad nacional pues, al ser un espacio sin fronteras, las posibilidades de los riesgos aumentan. Es cuando se necesita desarrollar métodos que puedan prevenir o controlar este nuevo entorno.

No significa que el ciberespacio sea un espacio sin normas o sin un aparato que lo regule. El ciberespacio se ha ido modificando gracias al apoyo de instituciones gubernamentales y privadas, pese a que estas mismas tienen un cierto control del ciberespacio, no todo la actividad interna la pueden regular o controlar, en especial cuando ya comienza a tener efecto en el espacio físico. El ciberterrorismo, las organizaciones de cibercrimen, los ciberataques (ciberoperaciones) a empresas e instituciones nacionales, ciberataques entre empresas o diferentes actores, el anonimato de internet, el robo de información, la suplantación de identidad, entre otros, son hechos que también llegaron a corromper el nuevo espacio.

Aunque la regulación se ha hecho con la participación de los usuarios, queda claro que existen retos al respecto. Los países han buscado actualizar sus sistemas jurídicos para poder adaptarse al nuevo cambio de las tecnologías y al rápido avance de los mismos. Se busca una regulación constante pero el problema siempre será que jamás van a la par, y cuando en el mundo físico se plantea un debate sobre alguna cuestión del ciberespacio, el ciberespacio ya ha desarrollado otros cuatro problemas más de los cuales preocuparse.

El ciberespacio, e Internet en especial porque es el medio en el que navegamos por él, ha permitido el desarrollo de las personas, los estados y en general de la dinámica internacional. A su vez, la globalización ha facilitado que la armonía entre el espacio físico y digital e igual que sus incompatibilidades. A lo largo de la historia de internet se ha buscado tener control de él. Los estados ya comienzan a crear estrategias de seguridad en el ciberespacio para que no exista ninguna forma de que su soberanía se vea vulnerada.

Pese a ello, han existido casos en donde los Estados han sido afectados por diferentes cuestiones. Desde ataques discretos (virus informáticos en computadoras personales) hasta la paralización de las funciones de un Estado

o la alerta de una planta nuclear. Es por estas cuestiones que los propios gobiernos, tanto a nivel nacional como internacional, más lo nacional que lo internacional, han acordado algunos convenios o leyes que permitan el control del ciberespacio. Las instituciones creadas para controlar las direcciones de internet o las infraestructuras que permiten el acceso a internet (los cables submarinos, por ejemplo). Han implementado normas, lineamientos, protocolos que puedan aportar algo para el uso de la red.

El capítulo 1 de esta investigación tuvo como propósito comprender los conceptos que construyen al ciberespacio a partir de la injerencia del Estado en este espacio. Este primer objetivo fue comprendido a partir de los conceptos ciberespacio e internet que actualmente se tiene en el análisis a nivel internacional. Es aquí cuando comienzan algunos de los problemas pues al no existir un consenso sobre los conceptos de base es cuando existen las diferencias al momento de querer concretar herramientas que controlen este nuevo espacio.

Para fines de esta investigación, se retoman los conceptos similares y que ayuda a darnos una base de lo que significa el ciberespacio. Se comprende como un medio virtual de interacción con efectos en el espacio físico. Pues este ha supuesto nuevos desafíos que ya no solo incumben a un solo país sino a todo el mundo conectado en él mismo. Sin distinción en sus distancias geográficas o fronteras políticas. Y son las personas un elemento protagónico al ser ellos quienes recrearon su realidad en este espacio obligando a las instituciones o empresas prestarle más atención.

Internet fue el medio que nos adentra al ciberespacio y este se convierte en el centro de la interacción humana. Ya los estudios comienzan alrededor del mismo, se reconstruyen el concepto de espacio donde ya no es solo el físico el importante sino un espacio virtual que tiene consecuencias en el real. El ciberespacio es el Espacio Virtual que se ha creado a partir de Internet donde toda la actividad humana ha ido trasformado para existir en las dos realidades.

Debido a estos nuevos elementos, el ciberespacio se convierte en un entorno que buscan controlar como se ha hecho en otros. Es por ello que las amenazas se convierten un factor importante en este espacio. La guerra y las confrontaciones comienzan a ser una realidad en este espacio que se transforma constantemente. Cualquier espacio que el ser humano conoce está

propenso a que se desencadene la guerra. El ciberespacio no se aleja de ello y todo comienza desde lo físico.

El ciberespacio depende de Infraestructuras importantes como los cables submarinos y los Proveedores de Servicio de Internet, por mencionar a los más importantes. En la cuestión de cables submarinos, su posicionamiento geográfico y los dueños de estos tienen que ver con intereses geopolíticos y económicos que mostrara sus efectos en el futuro. También su colocación en el mundo tiene efectos en la naturaleza y eso tendrá repercusiones en otros aspectos de la vida humana. En cuanto a los PSI, aquí podemos comprender a los dueños internet y la forma en que manejan a este mismo. Buscar el mayor dominio pero ya no solo los Estados pueden hacerlo, sino las empresas son los mayores competidores en este aspecto.

Aún así, los Estados no dejan de tener participación en el ciberespacio. Los Estados se constituyen a través de Infraestructuras Críticas que comienza a conectarlas al ciberespacio. Esto brinda una mayor innovación al Estado, se agiliza su funcionamiento pero también se convierte en una vulnerabilidad del mismo. Los ataques cibernéticos a Estonia en 2007 representaron una invasión a las IC de un Estado, y aunque en estos casos no hubo una invasión a las infraestructuras más importantes, si demostró las vulnerabilidades de un Estado y las obligaciones de seguridad no cumplidas por este.

Y aunque el caso de Estonia no fue el primer ejemplo de ciberataques, si fue el primer caso donde un Estado queda totalmente desconectado e incomunicado con el exterior. Esto se logra a partir de los ciberataques. Los ciberataques se dividen en diferentes categorías y con diferentes objetivos, con el fin de dañar a personas, entidades o instituciones. Los ataques pueden ir tanto contra los datos como con propósitos militares o comerciales.

En muchas ocasiones, estos ciberataques pueden formar parte de la estrategia de guerra de un Estado contra otro. Pues como se ha mencionado, el ciberespacio ha llegado a una injerencia tan grade que los Estados ya piensan en ciberejércitos, cibersoldados que combatirán como si fuese una guerra pero todo a través de internet. Y aunque aún existen muchos expertos renuentes a considerar la existencia de la ciberguerra, los eventos de los últimos años han probado que existe un enfrentamiento similar a la guerra

física con sus variaciones aunque todo debe seguir debatiéndose para comprender este fenómeno.

La ciberguerra se compone, de gran manera, de algunos elementos de la guerra física. Para poder establecer un buen criterio de la ciberguerra se debe partir del derecho de guerra implementado en el Derecho Internacional. Este derecho se forma a partir de los elementos de Ius ad Bellum y Ius in Bello. A partir de estos elementos, se debe considerar los elementos que conformen el concepto adecuado para la ciberguerra. Asimismo, es importante comprender los componentes que también son fundamentales para la protección del Estado en este tipo de eventos.

La ciberseguridad es el primer tema al respecto, al igual que todos los términos usados, no hay un consenso en su definición. De igual forma, para la investigación se entiende que es la aplicación de un proceso de análisis y gestión de riesgos en el uso de datos y sistemas basados en el ciberespacio. Al igual que en el espacio físico, la ciberseguridad es necesaria para los momentos de guerra y ciberataques. Para crear una de buena manera se necesita comprender la ciberdefensa y la ciberestrategia dentro del mismo.

Son términos similares a los usados en la seguridad física, solo que agregando el sufijo ciber para determinar que irán en función del ciberespacio. El plantear mecanismos de ciberseguridad, ciberdefensa y ciberestrategia que permitan la protección de las redes de los Estados. Han sido varios los casos en donde el Estado se vio vulnerable por diferentes ciberataques y determinó la importancia de la ciberseguridad. En especial en un mundo globalizado e interconectado que permite el desarrollo de escenarios conflictivos para el Estado.

A partir de la idea de que se necesitan nuevas medidas de seguridad para las amenazas que el ciberespacio ha traído al Estado, hay varios actores internacionales que han trabajado por su ciberseguridad. Y aunque es un tema que compete a todos los países que están en línea, son pocos los que realmente han presentado grandes iniciativas al tema y que pueden desarrollarse de forma positiva pero aún presentan varios obstáculos en el camino. El ejemplo de esto es la Unión Europea.

El capítulo 2 de esta investigación, tuvo como propósito describir las decisiones conjuntas que se han tomado en la Unión Europea para la

protección del ciberespacio y a partir de ellas retomar sus errores para comprender el porqué aún no ha creado mecanismos efectivos para la protección de su ciberespacio, en especial en los eventos de 2007.

Desde la publicación del Libro Verde de las Telecomunicaciones y la liberación de las mismas hasta la Estrategia de Seguridad Europea de 2016, la Unión Europea ha puesto en debate varios temas de interés sobre el ciberespacio. El problema, en la mayoría de sus propuestas, es que no ha encontrado un punto que le permita establecer medidas reales, además de la desunión de sus miembros y las diferencias de intereses políticos, la UE no ha logrado plasmar las características adecuadas que formen un concepto de seguridad apto para la Comunidad.

La UE necesita un concepto dinámico que pueda responder los posibles desarrollos a futuro y prevenir los ataques a sufrir, que aunque no son predecibles si pueden tener un impacto menor del que pueden llegar a ocasionar. De esa manera se podrá actuar de forma rápida, cosa que es necesario, y ya planteado, en la seguridad de la Unión Europea.

La participación de la UE en diferentes debates y propuestas sobre la regulación del ciberespacio, han logrado poner en tela de juicio la necesidad de actualizar normas jurídicas internacionales. Además, es necesaria la aclaración de los conceptos usados en el ciberespacio pues han sido parte de los impedimentos para determinar medidas ejecutables. El mayor problema que presenta la UE dentro de todas sus propuestas sobre la protección de IC; ciberespacio, y las telecomunicaciones en general, es que no existe un debate a profundidad que permita reconsiderar todos los temas a tratar con respecto al ciberespacio.

Si no se llega a un consenso entre los miembros de la UE que realmente pretenda la creación de medidas de ciberseguridad que prevengan la ciberguerra, los ciberataques, o el mismo ciberespacio, por muy avanzada que sea, la UE se quedará al margen de las protecciones del ciberespacio. Por ello, el Manual de Tallin es importante. Plantea temas antes no considerados por la UE y que podrían dar pie a que la Comunidad europea replantee una colaboración conjunta sobre estas cuestiones y cree una política de seguridad y defensa en el ciberespacio que responda a sus propios intereses.

El capítulo 3, se encarga de comprender todo el espectro del Manual de Tallin. Y analizar la influencia del Manual de Tallin en la construcción de una política de seguridad y defensa en la Unión Europea. Pues el Manual se ha convertido en un tema bastante debatible para las cuestiones del ciberespacio.

El Manual de Tallin, en su primera presentación, pretende regular la guerra. Esto no solo implica el acto de la ciberguerra sino todo lo que puede conllevar: uso de fuerza, la soberanía de los Estados, las estrategias nacionales de ciberseguridad, las funciones de los mismos Estados en estos eventos, entre otros. El Manual ha permitido plantear el debate que hacía falta a nivel internacional, plantear lo que es, en concreto, una legislación que competa a más de un Estado.

Si bien, la Unión Europea estaba ya planeando una regulación de forma regional, no estaba realmente plasmando los mecanismos reales que eran necesarios para la aplicación de leyes en el ciberespacio. Ni tampoco estaba comprometiéndose debido a la diferencia de intereses que su propia constitución implica. El Manual se plantea con un objetivo y no se pone a discutir los intereses estatales sino transformar los mecanismos legales ya planteados, que funcionan en un espacio, para ser aplicados en otro espacio. Esto permite comprender los errores que se vienen cometiendo desde que se crean las primeras leyes sobre el tema. No puedes crear leyes nuevas sino transformar las leyes que ya están, y sirven, para que puedan ser aplicables a otro espacio y funcionen.

Es claro que no van a tener los resultados similares que tuvieron en un espacio pero si plantean, o replantean, nuevos retos y nuevas cuestiones a debatir. Las insuficiencias estatales y los nuevos compromisos que llegará a tener el Estado con el espacio digital. Es por ello, que se ha planteado un Manual de Tallin 2.0: para conocer lo que ha escaseado en la primera versión. El segundo Manual se enfoca en las ciberoperaciones, y aún así existen deficiencias al respecto pero han permitido a los actores participantes, como la Unión Europea, plantear soluciones, u opciones, a acciones ya existentes para mejorarlas. Ese es el objetivo del Manual, un debate continuo y constante para su aplicación.

Su legalidad ha quedado siempre en la duda. Siendo países tan importantes los que participan en los debates es evidente que pueden

plantearse, de verdad, usarlo como legislación aplicable a nivel internacional pero, como se menciona en el párrafo anterior, no surge el Manual para ser aplicado sino para ser la guía de creación de las verdaderas leyes. Podría decirse que no aplicable hasta que se tenga una base más concreta y mayormente debatida sobre la legalidad del ciberespacio.

Asimismo, el aceptarlo, ahora, con tantos temas por ser debatidos, aplicaría a los Estados un compromiso mayor del que pueden manejar. Por eso es, en reiteradas ocasiones, que no es un Manual aplicable legalmente sino una guía porque el compromiso para controlar el ciberespacio aún no busca ser responsabilidad de nadie y no se quiere entorpecer la actividad del mismo. En especial con un actor como la Unión Europea en donde se busca digitalizar totalmente, como Estonia, para poder agilizar sus funciones y conectar más a sus miembros. Si se concibe un responsable de controlar el ciberespacio, se entorpece toda actividad y todos los propósitos planteados.

Y en primera instancia se compromete al Estado, y si el Estado se ve involucrado en la seguridad del ciberespacio, no permitirá que realmente se pueda desarrollar con la agilidad que ahora se desenvuelve por medio de internet. Regularizar también involucraría restringir y el ciberespacio se ha desarrollado para moverse con "libertad"[202] y esa es la base de los nuevos proyectos de la Unión Europea, libertad y conexión de las 28 economías.

Siendo la Unión Europea un actor compuesto por diferentes países se complica al momento de aplicación de un Manual. Por eso no es posible, se necesita un compromiso de todos los miembros por aplicarlo y un verdadero trabajo, quizá de más años, con el Manual para pensar usarlo como ley. Además, la UE busca proteger los intereses de todos sus socios, comerciales o políticos. Por ello es difícil crear un compromiso como aceptar un Manual propuesto por la OTAN. Agregando todas las relaciones inestables que la UE y la OTAN representan.

Pero no podría decirse que está del todo mal y que no es aplicable para la UE solo por sus intereses. Al final, es una base más sólida de lo que venía

[202] Me refiero más a la cuestión económica pues al no existir fronteras o restricciones reales, el comercio electrónico ha logrado manejarse con facilidad y ha agilizado todas las operaciones interbancarias. La UE está concentrada en este ámbito, en primer lugar, pues todos sus proyectos a futuro tienen que ver con la economía digital. Por ello, el conflicto con los derechos humanos y la crítica que tiene el Manual al respecto en donde no se hará distinción de objetivo civil o militar.

trabajando la Unión Europea. Si tiene fallos y necesita ampliar muchos aspectos legales, que quizá la UE ya ha trabajado, pero si permite a la Comunidad Europea, proponer directivas o supuestos que permitirían tener un manejo importante con el ciberespacio. Al igual que cualquier instrumento de guerra tiene que ser regulado pero debido a su amplio desarrollo y su impacto global, no solo es un actor al que le competen las cuestiones que se revisan del mismo y de ahí ese desarrollo débil en cuanto a su legislación.

Son muchas cuestiones a considerar para crear un marco regulatorio eficiente de estas políticas. Pues aunque la investigación se haya enfocado a las acciones de los Estados y los Organismos Internacionales más importantes, también existe el problema de las personas. En este caso el gran descontento de los europeos a muchas de las políticas sobre el internet propuestas por el Estado. Muchas de estas políticas se han construido a partir de medidas demasiado restrictivas y que acortan muchos de los principios de la libertad de expresión.

Internet es un sistema alejado de lo que se conoce en lo físico, es más sencillo para las personas imponer sus ideales y elegir las normas que quieren seguir. Por ello, en la mayoría de los casos, se ha optado por alejar, en lo mayor posible, a los Estados en la injerencia en el ciberespacio. Es quizá uno de los problemas más simples a tratar pero es fundamental entenderlo para saber qué ha detenido la aplicación de leyes en el ciberespacio.

Y no es que la sociedad este mal al exigir su derecho al ciberespacio, de hecho la filtración de información personal, el robo de identidad, o el mal manejo de su información personal son delitos que dañan la integridad de las personas en el ciberespacio y se debe exigir una solución pero es justamente el Estado el que tiene la obligación de dar esa respuesta.

Es un arma de doble filo, dónde se es necesario pero tampoco se quiere manera que controle todo lo que hacemos en el ciberespacio. Y aún así estamos vulnerables ante la cantidad de información nuestra que es guardada en la red. En una propuesta de lo que debería ser, se crearían políticas eficientes para la protección, tanto de las personas como de los intereses de los Estados para proteger sus redes pero eso no ocurrirá por el momento, en especial si no existen debates más profundos para la creación de estas políticas.

Es evidente la necesidad de plasmar muchas legislaciones existentes al ciberespacio pero tampoco se opta por profundizar en materia. El tercer capítulo desarrolla como es que el Grupo de Expertos se queda con la idea de guerra ya planteada pero no busca desarrollar sus propuestas a partir de un estudio más profundo del ciberespacio. La Deep Web, la instrusión de las redes sociales a la información personal de las personas, los virus informáticos, entre otras cuestiones, no están plasmadas en el Manual de Tallin porque no se consideran elementos de la guerra cuando aquí no hay que considerar los elementos que ya tenemos de la guerra sino adaptarla a los elementos del ciberespacio que pueden usarse para la ciberguerra.

Una cuestión a enfatizar en este capítulo, y que no es tomada, del todo, en cuenta, es la diferencia entre las doctrinas de seguridad de Estados Unidos y la Unión Europea pues es un capítulo que aborda un poco la diferencia de ideas en la cuestión de seguridad sin profundizar en sus doctrinas. Para Estados Unidos, la geopolítica estadounidense considera al Estado como el elemento primordial para las acciones en seguridad y defensa. Las acciones a seguir para Estados Unidos en protección de infraestructuras críticas, políticas de ciberseguridad o protección de territorio se basaran en que no repercuta al Estado

En cuanto a la Unión Europea, su preocupación principal es el ciudadano. Su enfoque es a partir del bienestar del ciudadano para construir políticas en cualquier ámbito. Por eso tenemos los términos y condiciones en las aplicaciones de las redes sociales, porque la ley europea obliga a las empresas multinacionales a implementarlas. Debido a la composición de esta idea de seguridad, se debe enfatizar el por qué se han alentado muchas de sus leyes o no han tenido la repercusión necesaria.

La cuestión de las personas es importante, sus derechos y mantener la libertad que les ha traído el internet es fundamental pero el Manual se ha desviado a legislar lo que ya se conoce sin estudiar el espacio que no tiene nada que ver con lo conocido. Y ese es el principal error del Manual de Tallin y que no parece buscar un análisis más profundo.

En cuanto al objetivo principal de la investigación de saber cuál es la política de seguridad y defensa en el ciberespacio para la Unión Europea a partir del Manual de Tallin podríamos concluir que es una que necesita mucho

trabajo y debate aún. Aún no podría decirse que ya existe porque aún hay revisiones, intereses y conflictos que la detienen.

La UE ya tiene las bases trabajadas para empezar a crear una política de Seguridad y Defensa en el Ciberespacio, uno de los obstáculos importantes que la detenía (Reino Unido) ya no estará y si los miembros se comprometen, en realidad, a construirla podrían tener éxito. Y el Manual de Tallin es la base para poder lograrlo de forma efectiva. El trabajo debe seguir, los debates deben seguir siendo continuos y para lograr el éxito se necesita ampliar los campos que se encargaran de ello.

ANEXOS

Debido a los derechos de autor, no se ha respetado el formato original de los documentos presentados.

ANEXO 1

NOTA:
Solo selecciono los 5 primeros puntos de la Directiva debido a que son los más sobresalientes pues señala los propósitos de la Unión Europea con esta propuesta. Que puede resumirse en la unificación económica de la UE a partir del Internet.

DIRECTIVA 2000/31/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 8 de junio de 2000

relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado constitutivo de la Comunidad Europea y, en particular, el apartado 2 de su artículo 47, y sus artículos 55 y 95,

Vista la propuesta de la Comisión [1],

Visto el dictamen del Comité Económico y Social [2],

De conformidad con el procedimiento establecido en el artículo 251 del Tratado [3],

Considerando lo siguiente:

(1) La Unión Europea tiene como objetivo crear una unión cada vez más estrecha entre los Estados y los pueblos europeos, así como asegurar el progreso económico y social. De conformidad con el apartado 2 del artículo 14 del Tratado, el mercado interior supone un espacio sin fronteras interiores, en el que la libre circulación de mercancías y servicios y la libertad de establecimiento están garantizadas. El desarrollo de los servicios de la sociedad de la información en el espacio sin fronteras interiores es un medio esencial para eliminar las barreras que dividen a los pueblos europeos.

(2) El desarrollo del comercio electrónico en la sociedad de la información ofrece importantes oportunidades para el empleo en la Comunidad, especialmente para las pequeñas y medianas empresas, que facilitará el crecimiento de las empresas europeas, así como las inversiones en innovación, y también puede incrementar la competitividad de la industria europea, siempre y cuando Internet sea accesible para todos.

(3) El Derecho comunitario y las características del ordenamiento jurídico comunitario constituyen una baza fundamental para que los ciudadanos y los agentes europeos puedan disfrutar plenamente, y sin tener en cuenta las fronteras, de las oportunidades que ofrece el comercio electrónico. La presente Directiva tiene, por consiguiente, como finalidad garantizar un elevado nivel de integración jurídica comunitaria con objeto de establecer un auténtico espacio sin fronteras interiores en el ámbito de los servicios de la sociedad de la información.

(4) Es importante que el comercio electrónico pueda beneficiarse plenamente del mercado interior y que se alcance un alto grado de integración comunitaria, como en el caso de la Directiva 89/552/CEE del Consejo, de 3 de octubre de 1989, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva [4].

(5) El desarrollo de los servicios de la sociedad de la información en la Comunidad se ve entorpecido por cierto número de obstáculos jurídicos que se oponen al buen funcionamiento del mercado interior y que hacen menos atractivo el ejercicio de la libertad de establecimiento y de la libre circulación de servicios. Dichos obstáculos tienen su origen en la disparidad de legislaciones, así como en la inseguridad jurídica de los regímenes nacionales aplicables a estos servicios; a falta de coordinación y ajuste de las legislaciones en los ámbitos en cuestión, hay obstáculos que pueden estar justificados con arreglo a la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas y existe una inseguridad jurídica sobre el alcance del control que los Estados miembros pueden realizar sobre los servicios procedentes de otro Estado miembro.

---

(1) DO C 30 de 5.2.1999, p. 4.
(2) DO C 169 de 16.6.1999, p. 36.
(3) Dictamen del Parlamento Europeo de 6 de mayo de 1999 (DO C 279 de 1.10.1999, p. 389), Posición común del Consejo de 28 de febrero de 2000 (DO C 128 de 8.5.2000, p. 32) y Decisión del Parlamento Europeo de 4 de mayo de 2000 (no publicada aún en el Diario oficial).

(4) DO L 298 de 17.10.1989, p. 23; Directiva cuya última modificación la constituye la Directiva 97/36/CE del Parlamento Europeo y del Consejo (DO L 202 de 30.7.1997, p. 60).

ANEXO 2

2.3. El Comité muestra su satisfacción por el hecho de que la propuesta aborde la cuestión de los criterios fundamentales para la concesión de las licencias. Como señala la Comisión, la concesión de licencias se ha convertido en algunos casos en un procedimiento muy costoso y que básicamente no reporta beneficio alguno al usuario final. Sólo puede lograrse un mercado único europeo si se armoniza la concesión de licencias en un nivel de intervención bajo, que ha demostrado su eficacia en varios Estados miembros.

2.4. Es importante que las condiciones para autorizar las operaciones no incluyan obligaciones no específicas del sector. El Comité muestra su satisfacción por el hecho de que se especifique así en el artículo 6 de la Directiva. Asimismo, acoge positivamente que el considerando (14) exprese claramente que no es necesario exigir de manera sistemática y regular una prueba del cumplimiento de todas las condiciones. Se trata de un paso positivo para reducir la carga normativa de las empresas.

2.5. El CES comparte la opinión de la Comisión de que las licencias sólo deberían usarse cuando haya escasez del espectro radioeléctrico y de números de teléfono y que las tasas administrativas no deberían rebasar los costes administrativos de la regulación mínima propuesta. Aparentemente, crece la preocupación de que los usuarios de las tecnologías de la información se vean obligados a contribuir al pago de costes de las licencias del espectro que exceden en gran medida los meros costes administrativos y que no tienen nada que ver con los establecidos mediante subasta.

2.6. En opinión del Comité, la propuesta de Directiva sobre autorización debería modificarse para prohibir explícitamente la práctica, cada vez más común, de percibir cánones únicos que no se usan para propósitos que puedan incrementar la eficacia del espectro ni forman parte del procedimiento de subasta ni de ningún otro sistema en el que el precio se utiliza como medio para lograr la eficacia de la propia distribución del espectro.

Bruselas, el 24 de enero de 2001.

El Presidente

del Comité Económico y Social

Göke FRERICHS

Dictamen del Comité Económico y Social sobre la «Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas»

(2001/C 123/13)

El 16 de octubre de 2000, de conformidad con el artículo 95 del Tratado constitutivo de la Comunidad Europea, el Consejo decidió consultar al Comité Económico y Social sobre la propuesta mencionada.

La Sección de Transportes, Energía, Infraestructuras y Sociedad de la Información, encargada de preparar los trabajos en este asunto, aprobó su dictamen el 7 de diciembre de 2000 (ponente: Sr. Lagerholm).

En su 378ºPleno de los días 24 y 25 de enero de 2001 (sesión del 24 de enero de 2001), el Comité Económico y Social ha aprobado por 77 votos a favor y 1 abstención el presente Dictamen.

1. Introducción

1.1. Desde 1990, la Comisión Europea ha ido estableciendo progresivamente un marco regulador integral para la liberalización del mercado de las telecomunicaciones. Esto ha sido de importancia vital para la competitividad global de la Unión Europea. Disponer de una industria de comunicaciones avanzadas constituye una condición previa para la transición de Europa a la sociedad de la información. En la reunión de los días 23 y 24 de marzo de 2000 del Consejo Europeo de Lisboa se subrayaron las perspectivas de crecimiento, competitividad y creación de puestos de trabajo que ofrece el paso a una economía digital y basada en el conocimiento. En particular, el Consejo insistió en la importancia de que las empresas y los ciudadanos de Europa puedan acceder a una infraestructura de comunicaciones de primera línea y poco costosa, así como a una amplia gama de servicios.

1.2. El actual marco regulador de las telecomunicaciones ha conseguido crear las condiciones necesarias para una competencia efectiva en el sector de las telecomunicaciones a lo largo de la transición del régimen de monopolio al de libre competencia. El nuevo marco regulador para la infraestructura de comunicaciones y servicios asociados debe estar dedicado a partir de ahora a promover y apoyar un mercado europeo abierto y competitivo para los servicios de comunicaciones, a beneficiar al ciudadano europeo y a consolidar el mercado interior.

2. La propuesta de la Comisión

2.1. La convergencia de los sectores de telecomunicaciones, medios de comunicación y tecnologías de la información [1] supone que todos los servicios y las redes de transmisión estén sometidos a un único marco regulador. El marco regulador propuesto debe constar de la Directiva sometida a examen y, además, de las siguientes medidas:

— Directiva relativa a la autorización de las redes y los servicios de comunicaciones electrónicas,

— Directiva relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados y a su interconexión,

— Directiva relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas,

— Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas,

— Reglamento sobre el acceso desagregado al bucle local.

2.1.1. Junto a las medidas mencionadas está también la propuesta de Decisión relativa a un marco regulador de la política del espectro radioeléctrico en la Comunidad.

2.1.2. Las propuestas se basan en una consulta pública acerca del Libro Verde sobre la convergencia, el Libro Verde sobre la política en materia de espectro radioeléctrico [2] y la Revisión de 1999 [3] del actual marco regulador.

2.2. El Artículo I de la propuesta de Directiva expone la finalidad y el ámbito de aplicación del nuevo marco: establecer un marco armonizado para la regulación de las redes y los servicios de comunicaciones electrónicas, esto es, incluyendo todas las redes satelitales y terrenales, tanto fijas como inalámbricas.

2.3. En el capítulo II se modifican los principios para el establecimiento de las autoridades nacionales de reglamentación (ANR), así como determinados procedimientos a los que están sometidas. Los Estados miembros garantizarán la independencia de las ANR y publicarán las misiones que les corresponden. La Directiva establece un derecho de recurso y deja claro que deberá ejercerse ante un organismo independiente de la administración. Se establece el derecho de una ANR a recabar información de los agentes del mercado para desempeñar su misión con eficacia. Las autoridades nacionales de reglamentación deberán consultar con todas las partes interesadas las decisiones propuestas y hacer uso de sus atribuciones de modo imparcial y transparente.

2.4. De conformidad con el capítulo III, es tarea de las ANR fomentar, de manera neutra con respecto a la tecnología, un mercado abierto y competitivo, contribuir al desarrollo del mercado interior y promover los intereses de los ciudadanos europeos. Fomentarán la armonización del uso del espectro radioeléctrico a escala comunitaria y estarán encargadas de su eficaz administración y de la atribución y asignación de espectro radioeléctrico basándose en criterios objetivos, transparentes, no discriminatorios y proporcionales. Deberá contarse, además, con procedimientos rápidos y no discriminatorios para el otorgamiento de derechos de paso y, en algunas circunstancias, podría resultar adecuado imponer la obligación de compartir instalaciones.

2.5. Las disposiciones generales del capítulo IV son aplicables a varias de las directivas del nuevo marco legislativo. De conformidad con dicho capítulo, se considerará que una empresa tiene peso significativo en el mercado si, individual o conjuntamente con otras, disfruta de una posición de fuerza económica que permite que su comportamiento sea, en medida apreciable, independiente de los competidores, los clientes y, en última instancia, de los consumidores.

---

[1] «Libro Verde sobre la convergencia de los sectores de telecomunicaciones, medios de comunicación y tecnologías de la información y sobre sus consecuencias para la reglamentación en la perspectiva de la sociedad de la información» (COM(97) 623 final); Dictamen del CES en el DO C 214 del 10.7.1998.

[2] «Los próximos pasos en la política del espectro radioeléctrico — Resultados de la consulta pública sobre el Libro Verde» (COM(1999) 538 final); Dictamen del CES sobre el Libro Verde, DO C 169 del 16.6.1999.

[3] «Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones — Hacia un nuevo marco para la infraestructura de comunicaciones electrónicas y los servicios asociados — Revisión de 1999 del sector de las comunicaciones» (COM(1999) 539 final); Dictamen del CES, DO C 204 de 18.7.2000. «Comunicación de la Comisión — Resultados de la consulta pública sobre la Revisión de 1999 del sector de las comunicaciones y las orientaciones para el nuevo marco regulador» (COM(2000) 239 final); Dictamen del CES, DO C 14 de 16.1.2001.

2.6. En los mercados de dimensión internacional, enumerados en la Decisión que deberá adoptar la Comisión sobre mercados de productos y servicios pertinentes, se realizarán análisis del mercado regulares. Cuando una autoridad nacional de reglamentación determine que uno de los mercados no es realmente competitivo en una zona geográfica específica, impondrá las obligaciones reglamentarias sectoriales establecidas en las Medidas específicas, o mantendrá dichas obligaciones si ya existen.

2.7. Otras disposiciones hacen referencia a la normalización o la resolución de litigios entre empresas y partes de distintos Estados miembros. A fin de lograr la armonización del mercado interior, la Comisión podrá formular recomendaciones y adoptar medidas vinculantes de armonización utilizando procedimientos de comitología. Estará asistida por el Comité de Comunicaciones. La Directiva marco crea también el Grupo de Alto Nivel de Comunicaciones con carácter consultivo y que actuará con independencia.

3. Observaciones generales

3.1. El desarrollo de la tecnología de la información (TI) y del sector de las telecomunicaciones ha sido impresionante en Europa en la última década. Los clientes europeos no siempre disfrutan de las tarifas más bajas, pero en la mayoría de los Estados miembros pueden elegir servicios que se adecuan a sus necesidades hasta un punto que no encuentra apenas parangón en el resto del mundo. En la mayor parte de los países las tarifas están descendiendo rápidamente.

Esto ha sido posible básicamente gracias a los cambios tecnológicos, pero estas oportunidades no podrían haber supuesto una ventaja para el usuario final si la normativa sobre telecomunicaciones de la UE no hubiera abierto el camino a la competencia al suprimir los monopolios históricos y otros derechos especiales.

Aunque está claro que la transición total desde una forma monopolística de suministro a una competitiva no ha terminado todavía en todos los Estados miembros ni en todos los mercados importantes, resulta cada vez más evidente que el marco regulador de la década de los noventa no es lo suficientemente flexible en relación con los rápidos cambios del mercado, cambios que implican la mejora de los productos y servicios existentes y la creación de otros nuevos, en parte debido a la convergencia de las tecnologías.

3.2. El Comité Económico y Social, en su Dictamen sobre la Comunicación de la Comisión sobre la Revisión de 1999 [1], expresaba su apoyo general a la propuesta de nuevo marco legislativo en materia de comunicaciones electrónicas.

3.2.1. El Comité acogía

«con especial entusiasmo la iniciativa de basar la reglamentación propuesta en los aspectos siguientes:

— el fomento y apoyo de un mercado europeo abierto y competitivo;

— la consolidación de un mercado interior;

— un mayor recurso al derecho de competencia y la simplificación y reducción de la legislación específica del sector junto con recomendaciones, orientaciones y acuerdos sectoriales. Aparte de regular el acceso a los recursos limitados, es necesario aplicar una regulación específica del sector, aunque sólo en ámbitos en los que la competencia sea insuficiente y únicamente de forma provisional;

— la neutralidad tecnológica, que implica, entre otros aspectos, que no se apliquen medidas específicas a Internet. Sin embargo, una regulación que aspira a la neutralidad tecnológica no debe tender a una normalización demasiado estricta de los servicios nuevos, sino más bien a la desarticulación de la anterior reglamentación específica de los servicios tradicionales.»

3.2.2. El Comité subrayaba que «a medida que la Comisión vaya desarrollando en detalle sus propuestas, se deberá poner especial atención en el cumplimiento de estos principios. Asimismo, es preciso velar por que la aplicación de estas propuestas no se efectúe al ritmo de los Estados miembros más lentos, sino que es preferible sustituir la regulación de un sector específico por un derecho de competencia general en los distintos mercados (geográficos y de servicios) a medida que se vaya asentando la competencia. Puede que este asunto se complique con la ampliación de la UE; habrá entonces que proporcionar un apoyo adecuado a los nuevos países miembros.»

3.2.3. El Comité también hacía hincapié en «el carácter global de los mercados de comunicación en proceso de convergencia. El marco regulador europeo que se propone no debe considerarse independientemente de su contexto. Es de vital importancia que se mantenga la competitividad de los operadores europeos y que se les permita desarrollarse. A este respecto, existe un riesgo de que la regulación regional lleve a que el mercado regional europeo se quede aislado del mercado global, especialmente si se permite que una amplia regulación impida el desarrollo de las fuerzas del mercado. Por esta razón el Comité insta a la Comisión a que tenga en cuenta las consecuencias de cada medida en la competitividad global de la industria europea.»

[1] «Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones — Hacia un nuevo marco para la infraestructura de comunicaciones electrónicas y los servicios asociados — Revisión de 1999 del sector de las comunicaciones» (COM(1999) 539 final); Dictamen del CES, DO C 204 de 18.7.2000. «Comunicación de la Comisión — Resultados de la consulta pública sobre la Revisión de 1999 del sector de las comunicaciones y las orientaciones para el nuevo marco regulador» (COM(2000) 239 final); Dictamen del CES, DO C 14 de 16.1.2001.

3.3. El CES acoge con satisfacción el hecho de que la Comisión haya mantenido el esquema general del marco regulador presentado tras la amplia consulta pública sobre la Revisión de las Comunicaciones efectuada en 1999.

3.3.1. El Comité considera adecuado y oportuno el principio de una legislación cada vez más flexible con un limitado número de salvaguardias públicas que caracteriza a las Directivas presentadas actualmente. También recomienda que el nuevo marco tenga como objetivo la capacidad de predecir y una mayor correspondencia con la legislación horizontal de la UE sobre competencia y protección del consumidor.

3.4. El Comité insiste en la importancia de alinearse rápidamente con los principios horizontales. El calendario propuesto por la Comisión no debe acortarse aún más por motivos institucionales o prácticos. No obstante, en relación con la evolución real de la técnica y del mercado podría resultar demasiado lento y contrarrestar la ventaja competitiva de que dispone actualmente el sector europeo de las comunicaciones electrónicas.

3.5. El Comité suscribe el objetivo de la Comisión de introducir un marco regulador único para las redes y servicios de comunicación en la UE. Sin embargo, existen algunos aspectos concretos en las diferentes propuestas de Directiva que el CES no puede respaldar.

3.6. En algunos puntos se hacen afirmaciones que parecen ser contradictorias o no estar en sintonía con las directrices generales. El Comité se ocupa de estos puntos en su dictamen sobre las respectivas directivas.

4. La Directiva marco

4.1. El CES acoge con satisfacción que la Directiva marco se plantee tratar únicamente los casos en que la competencia efectiva no funcione bien en un mercado de referencia. Asimismo, valora positivamente el hecho de que se aplique la misma definición de mercado de referencia que en las normas de competencia de la UE. Existe una gran experiencia con esta práctica y el resultado se puede prever con relativa certeza.

4.2. Un asunto que se debe debatir en los Estados miembros es si el resultado del análisis del mercado de referencia da lugar a una normativa de la competencia *ex ante* o a la tradicional *ex post*. Son muchos los que están a favor de que la legislación *exante* se aplique únicamente a las empresas que tienen su posición dominante en el mercado en virtud de que financian la inversión de un régimen monopolístico. Esto parece estar en la misma línea que los argumentos de la Comisión que se reflejan en el texto (considerando 20) de la Directiva propuesta. En opinión del Comité, este extremo debería reflejarse también explícitamente en la propia Directiva.

4.3. Se podría argumentar que el procedimiento inverso de intervención reguladora, cuándo se debe suspender temporal o permanentemente la aplicación de una legislación determinada si se ha logrado su objetivo, debería estar subrayado más explícitamente en la Directiva marco. Para el consumidor final o para los proveedores de servicios es igualmente importante que la legislación deje de ser de aplicación una vez que se ha logrado su objetivo. En este caso tiene que existir un margen de estabilidad en la aplicación.

4.4. Se propone que las obligaciones existentes se plasmen en un régimen nuevo para las empresas con un peso significativo en el mercado (PMS). En opinión del Comité, en ese caso debe quedar claramente especificado que la legislación vigente sólo se podrá aplicar hasta que se concluya el primer análisis de mercados de referencia de acuerdo con la nueva Directiva. Esto debería de quedar claro en la propuesta de Directiva marco.

4.5. Una cuestión muy importante es la posibilidad de predicción. El recurso a las normas de competencia tiende a fomentar la posibilidad de predicción, pero la experiencia hasta ahora demuestra que la aplicación de un marco regulador común puede dar lugar a interpretaciones muy diferentes en los Estados miembros, como lo demuestra la notificación de PMS en los mercados de comunicaciones móviles. La telefonía era, sobre todo, un servicio doméstico mientras que los nuevos servicios de TI están cruzando fronteras rápidamente y requieren una interpretación más armonizada que la que ha proporcionado el actual régimen.

4.6. El CES apoya, por lo tanto, el principio de hacer una lista de las intervenciones aceptables de las autoridades nacionales de reglamentación (ANR) y la notificación obligatoria de acciones reguladoras propuestas en los Estados miembros de conformidad con el artículo 6. Ahora bien, se podría poner en duda si la consulta total a todos los Estados miembros es compatible en la práctica con la rapidez que requiere la legislación sobre TI. El problema se puede acentuar considerablemente con la ampliación de la Unión y pueden aumentar las diferencias entre los diferentes sectores de la comunicación de los Estados miembros. Se debe considerar, pues, cuidadosamente si el procedimiento normal de armonización de las medidas reguladoras se puede estructurar de manera que las medidas se deban comunicar únicamente a la Comisión.

4.7. El Comité también muestra su preocupación por el hecho de que, por ejemplo, según el artículo 14, la Comisión está obligada formalmente a consultar únicamente a las ANR. Considera necesario que también se consulte a los consumidores y a las empresas de una forma coherente con la brevedad de los plazos exigida. El Comité manifiesta su preocupación con respecto al apartado 6 del artículo 14 de la Directiva, en virtud del cual la Comisión puede modificar o suspender toda decisión de una autoridad nacional de reglamentación.

4.8. De acuerdo con la Directiva marco, la Comisión tiene derecho —al menos, temporalmente— apoyándose en los artículos mencionados más arriba, a impedir la aplicación de una decisión de las autoridades nacionales sobre las medidas y en asuntos de gestión del espectro radioeléctrico. Esta limitación de derechos de decisión de los Estados miembros viene motivada por la importancia fundamental de las definiciones del mercado y su interconexión con el funcionamiento del mercado interior. Según el principio de subsidiariedad, el nivel comunitario es el más adecuado para tomar estas decisiones. Pero obviamente el artículo debe aplicarse de una manera razonable y de conformidad con el principio de proporcionalidad. No se debe ampliar más a otras medias reguladoras.

4.8.1. Cuando la adjudicación de licencias de utilización del espectro radioeléctrico, de conformidad con el apartado 6 del artículo 8, esté sujeta al procedimiento previsto en el artículo 6; será necesaria una definición más clara para determinar en qué medida los intercambios de derechos poseen tales implicaciones transfronterizas que impiden gestionarlos mejor a nivel local. La mayoría de las licencias de frecuencias deberían aplicarse a la utilización dentro de un Estado miembro sin que ello tenga consecuencias fundamentales para el conjunto de la UE. Para resolver de manera práctica los posibles problemas de interferencias en las regiones fronterizas existe un procedimiento internacional eficaz que se basa en el reglamento de radiocomunicaciones de la UIT. El procedimiento previsto en el artículo 6 debe limitarse pues a determinados ámbitos de la competencia en telecomunicaciones en su conjunto como GSM o UMTS.

4.9. La formulación del artículo 4 sobre el derecho a recurrir la decisión de las autoridades nacionales de reglamentación no parece demasiado clara sobre un aspecto muy importante. El apartado 1 del artículo 4 establece, entre otras cosas, que mientras se resuelven los recursos, «prevalecerá la decisión de la autoridad nacional de reglamentación». Debería quedar claro que esto no debe influir en la posibilidad de que una parte afectada pueda aplazar la suspensión de una medida decidida por una ANR mientras que esté pendiente en los tribunales el litigio, si dicho procedimiento de inhibición existe en el Estado miembro.

4.10. El Comité se congratula de que la Comisión se proponga aplicar el principio de la neutralidad tecnológica, pero quiere subrayar que no es fácil lograrla a corto plazo.

4.10.1. La neutralidad tecnológica no debe significar transferir a nuevas áreas medidas reguladoras diseñadas para los servicios tradicionales. En opinión del Comité, la propuesta de reglamentación de la interconexión es un ejemplo de que puede dar lugar a distorsiones.

4.10.2. La reglamentación de la interconexión surge a partir de la telefonía, que es un servicio de transmisión normalizado con terminales de usuario normalizadas. En este caso es fácil definir la interconexión, todo el mundo puede conectarse y estar conectado al servicio telefónico independientemente de la red de telefonía de la que dependa. Para que se puedan desarrollar nuevos servicios basados en el servicio telefónico es preciso que el telefax, por ejemplo, esté incluido en la interconexión.

4.10.3. Los servicios basados en el protocolo de Internet (PI), y especialmente la propia Internet, no están definidos de manera clara y limitada, como en el caso de la telefonía, y no pueden ser elegidos por los clientes. En relación con los servicios PI, dependiendo de la modalidad de uso los clientes eligen un acceso diferente. Un cliente puede disponer de un teléfono UMTS o un ordenador para comunicarse en la red. Los clientes pueden estar conectados a la red telefónica vía módem o a una red de banda ancha con una capacidad de 10-20 veces mayor. Pagar una costosa banda ancha sólo se justifica cuando se está dispuesto a pagar por cargar en el ordenador servicios como películas cinematográficas. Para la «navegación normal» es suficiente con la décima parte de la capacidad necesaria para las películas.

4.10.4. En el entorno PI no se da la semejanza fundamental existente en las redes de telefonía sobre las cuales se ha construido el concepto de interconexión. No todos los servicios PI se pueden transmitir a todos los servicios de comunicación electrónica puesto que su capacidad puede variar considerablemente. Las redes con menor capacidad se bloquearían en el caso de que se introdujera la interconexión obligatoria. La alternativa sería una ampliación que resultaría muy costosa.

4.10.5. No obstante, en opinión del Comité, la falta de legislación sobre interconexión no debería plantear demasiados problemas. En la mayoría de los Estados miembros se está produciendo un rápido desarrollo de estructuras de banda ancha paralelas en competencia entre sí. Los propietarios de estas estructuras tienen un gran interés económico en atraer a ellas mediante un sistema abierto, todo el tráfico posible. El sistema abierto es además una de las exigencias del usuario de Internet. Más bien parece que existe el peligro de que determinadas infraestructuras nuevas compitan deslealmente confiándose en la reglamentación específica aún vigente, por ejemplo, en el sector de la distribución eléctrica o de la comunicación física, a que se deba limitar el flujo de información electrónica.

4.10.6. Evidentemente, los nuevos mercados en rápida expansión y los de las redes de banda ancha pueden presentar en algún momento un verdadero falseamiento de la competencia que podría dar lugar desde un punto de vista formalista, estrecho y estático al estatuto de operador PMS. Si esto a su vez fuera utilizado como justificación para exigir la orientación de los impuestos en función de los costes, el Comité considera que se correría el riesgo de reducir la voluntad de inversión y de poner en peligro la competencia a largo plazo. Es importante darse cuenta de que las relaciones en estos nuevos mercados se caracterizan por una diferencia dominante en relación con el marco de referencia de la noción de interconexión —la telefonía fija tradicional— en el que la mayor parte de las inversiones en red ya se han hecho y que la reglamentación se basa en aprovechar lo mejor posible los valores históricos.

Bruselas, el 24 de enero de 2001.

El Presidente
del Comité Económico y Social
Göke FRERICHS

Dictamen del Comité Económico y Social sobre la «Propuesta de Decisión del Parlamento Europeo y del Consejo sobre un marco regulador de la política del espectro radioeléctrico en la Comunidad Europea»

(2001/C 123/14)

El 4 de octubre de 2000, de conformidad con el artículo 95 del Tratado constitutivo de la Comunidad Europea, el Consejo decidió consultar al Comité Económico y Social sobre la propuesta mencionada.

La Sección de Transportes, Energía, Infraestructuras y Sociedad de la Información, encargada de preparar los trabajos en este asunto, aprobó su dictamen el 9 de enero de 2001 (ponente: Sr. Hernández Bataller).

En su 378º Pleno de los días 24 y 25 de enero de 2001 (sesión del 24 de enero de 2001) el Comité Económico y Social ha aprobado el presente Dictamen por 80 votos a favor, 1 en contra y 1 abstención.

1. Introducción

1.1. El uso intensivo del espectro radioeléctrico, el complejo proceso decisorio para su atribución y asignación, la enorme expansión mundial como consecuencia de la convergencia tecnológica de diversos servicios y la evolución económica, así como la necesidad de cumplir los principios del mercado interior y proteger los intereses comunitarios a nivel internacional, han sido, entre otras, las causas por las que las instituciones comunitarias se han preocupado de dicha materia.

1.2. El Libro Verde sobre «la política en materia de espectro radioeléctrico en el contexto de las políticas de telecomunicaciones, radiodifusión, transporte e I+D de la Comunidad Europea» [1] abordaba cinco cuestiones claves:

- la planificación estratégica de la utilización del espectro radioeléctrico;
- la armonización de la atribución de espectro radioeléctrico;
- la asignación de espectro radioeléctrico y concesión de licencias;
- los equipos radioeléctricos y la normalización;
- el marco institucional para la coordinación del espectro radioeléctrico.

1.3. El mencionado Libro Verde fue acogido favorablemente por el Comité Económico y Social, al considerar que el espectro radioeléctrico es la columna vertebral de un amplio abanico de importantes sectores industriales, y que en el futuro, además de las razones técnicas, las decisiones tendrán que reflejar la importancia económica, social y política del uso del espectro.

[1] COM(1998) 596 final; Dictamen del CES del 16 de junio de 1999, DO C 169.

ANEXO 3

Nuevo marco para los servicios de comunicaciones electrónicas

1) OBJETIVO

Presentar una revisión de la legislación comunitaria en materia de telecomunicaciones y proponer los elementos principales de un nuevo marco regulador para la infraestructura de comunicaciones y los servicios asociados.

2) ACTO

Comunicación de la Comisión, de 10 de noviembre de 1999, al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. Hacia un nuevo marco para la infraestructura de comunicaciones electrónicas y los servicios asociados. Revisión de 1999 del marco regulador de las comunicaciones [COM (1999) 539 final, 10.11.1999 - no publicada en el Diario Oficial].

3) SÍNTESIS

La liberalización del mercado europeo de las telecomunicaciones culminó el 1 de enero de 1998 con la liberalización total de todas las redes y servicios de telecomunicaciones en prácticamente todos los Estados miembros de la Unión Europea. El progreso tecnológico, la innovación en la oferta de servicios, la rebaja de los precios y las mejoras de la calidad producidos por la introducción de la competencia en el sector de las telecomunicaciones constituyen la base para la transición en Europa a la sociedad de la información. La convergencia de los sectores de telecomunicaciones, la radiodifusión y las tecnologías de la información está dando una configuración nueva al mercado de las comunicaciones, incluida la convergencia de las comunicaciones fijas, móviles, terrestres y por satélite, y la convergencia de los sistemas de comunicaciones y de localización. En lo que se refiere a la infraestructura de comunicaciones y servicios asociados, la convergencia tiene por efecto que la separación tradicional de las funciones reguladoras de estos sectores sea cada vez más obsoleta y esté reclamando un régimen regulador coherente.

En este contexto, la presente comunicación emprende una revisión del marco regulador de las comunicaciones vigente en respuesta a la necesidad de un planteamiento más horizontal de la regulación de la infraestructura de comunicaciones puesta de manifiesto en la consulta sobre la convergencia. Tiene en cuenta asimismo las ideas esenciales planteadas, por ejemplo, en la consulta a propósito del Libro Verde sobre el espectro radioeléctrico, el informe sobre el desarrollo del mercado de la televisión digital en la Unión Europea y el 5º informe sobre la aplicación del paquete regulador de las telecomunicaciones.

Son cinco los principios en que se basará el nuevo marco regulador y que gobernarán la actuación reguladora a escala comunitaria y nacional. Establecen que la regulación futura debe:

- responder a objetivos políticos claramente definidos;

- reducirse al mínimo posible para alcanzar estos objetivos (por ejemplo, mediante la introducción de mecanismos destinados a reducir aún más la reglamentación cuando la competencia permita alcanzar los objetivos políticos);
- mejorar la seguridad jurídica en un mercado dinámico;
- aspirar a la neutralidad tecnológica (no imponer un tipo particular de tecnología ni discriminar en favor del uso de un tipo particular de tecnología, sino garantizar que la prestación de servicios sea regulada de forma homogénea y con independencia de la infraestructura de comunicaciones a través de la que se presten estos servicios);
- aplicarse al nivel más próximo posible a las actividades reguladas (aunque haya sido consensuada a nivel mundial, regional o nacional).

Teniendo en cuenta estos cinco principios, la Comisión prevé estructurar el nuevo marco regulador en torno a las líneas generales siguientes:

- una normativa comunitaria específica de los sectores convergentes. Consistirá en una Directiva marco en la que se establecerán los objetivos políticos generales y específicos y cuatro directivas particulares sobre concesión de licencias, acceso e interconexión, servicio universal y protección de datos y de la intimidad (lo que representará una simplificación considerable del marco actual, dado que los veinte instrumentos legislativos existentes se reducen a seis);
- medidas de acompañamiento no vinculantes;
- normas de competencia: mayor recurso a las normas generales que regulan la competencia, que irá sustituyendo a gran parte de la normativa sectorial a medida que la competencia se haga más eficaz.

De forma paralela, las directivas derivadas del artículo 86 del Tratado se simplificarán y codificarán en una única norma jurídica.

Sobre la base de estos principios generales, la presente Comunicación define la posición provisional de la Comisión con respecto a cada uno de los diferentes ámbitos de su política reguladora e invita a las partes interesadas a pronunciarse al respecto antes del **15 de febrero de 2000**. A la luz de las observaciones que reciba, la Comisión se propone presentar propuestas de modificación del marco regulador vigente en el curso del primer semestre de 2000.

Por lo que respecta a la normativa vinculante específica del sector, el futuro marco regulador prevé la elaboración de una nueva Directiva marco que, entre otras cosas, deberá:

- definir los objetivos políticos concretos que deben de alcanzar los Estados miembros;
- garantizar los derechos específicos de los consumidores (por ejemplo, procedimientos de arreglo de controversias, números de llamada de urgencia, mejora de la transparencia y del acceso a la información, etc.);
- garantizar un nivel apropiado de interoperabilidad para los servicios y los equipos de comunicaciones;
- establecer los derechos y las responsabilidades y las facultades y procedimientos de toma de decisión de las ANR (Autoridad nacional de reglamentación);
- definir y establecer normas de funcionamiento para el nuevo Comité de comunicaciones y para el Grupo de alto nivel sobre las comunicaciones.

La Directiva marco irá acompañada de **cuatro Directivas específicas** basadas en el artículo 95 del Tratado:

- Directiva sobre autorizaciones y licencias (que incluirá normas para la gestión eficaz de los recursos escasos y el acceso a los mismos);

- Directiva sobre la prestación del servicio universal, que incluirá elementos de las actuales directivas sobre telefonía vocal e interconexión;
- Directiva sobre acceso e interconexión (basada en la vigente Directiva sobre interconexión y en la Directiva sobre normas de televisión);
- Directiva sobre tratamiento de datos y protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva actualizada y clarificada para incorporar el progreso tecnológico).

El Derecho de competencia irá adquiriendo cada vez más importancia en el sector hasta sustituir la parte esencial de la regulación sectorial a medida que la competencia se instale definitivamente en el mercado.

La presente Comunicación propone también cambios substanciales de la legislación vigente que permitan abordar los problemas a que debe enfrentarse el nuevo marco regulador.

Estos cambios se refieren a los aspectos siguientes:

Licencias y autorizaciones

La Comisión insiste en la necesidad de reducir las trabas administrativas al acceso para impulsar un mercado europeo competitivo de los servicios de telecomunicaciones.

En concreto, la Comisión propone:

- utilizar las autorizaciones generales como base para la concesión de licencias a las redes y servicios de comunicaciones, reservando las autorizaciones específicas a la atribución del espectro radioeléctrico y de los números;
- aplicar un marco político completo y coherente a las infraestructuras de comunicaciones, incluidas las redes de radiodifusión;
- garantizar que los cánones o derechos por las autorizaciones cubran sólo los costes administrativos justificados y pertinentes;
- continuar autorizando los servicios de comunicaciones que utilizan la Internet de modo equivalente a otros servicios de comunicaciones (es decir, sin regulación específica para Internet).

Acceso e interconexión

En la legislación comunitaria, el 'acceso' es un concepto genérico que abarca todas las formas de acceso a las redes y servicios de dominio público, mientras que el término 'interconexión' se refiere al enlace físico y lógico entre redes. Las normas de acceso e interconexión garantizan la interoperabilidad y son fundamentales para garantizar el establecimiento de la competencia. La Comisión reconoce la importancia crítica que tiene la provisión de servicios de acceso e interconexión y, por tanto, propone lo siguiente:

- mantener las medidas comunitarias específicas que regulan el acceso y la interconexión, basándose en los principios establecidos en la Directiva sobre interconexión y en la Directiva sobre normas de señales de televisión;
- en cuanto al acceso a las infraestructuras de redes, dar a las ANR la responsabilidad de resolver los temas específicos de acceso; exigir a los titulares de infraestructuras con un peso significativo en el mercado que negocien, según términos comerciales, las solicitudes de acceso; mantener la posibilidad de la intervención de las ANR para el arreglo de controversias;
- en cuanto a la interconexión, mantener el requisito de la interconexión orientada a los costes contemplado en las directivas (disposiciones jurídicas), pero interpretar este concepto mediante recomendaciones de la Comisión;

- elaborar, cuando así convenga, recomendaciones sobre acceso, en particular considerar la conveniencia de formular una recomendación a los Estados miembros sobre los aspectos técnicos y económicos del acceso desglosado al bucle local (el bucle local es el enlace entre las dependencias del usuario y la red de telecomunicaciones). La Comisión considera que la disponibilidad del acceso desglosado al bucle local reforzaría la competencia y permitiría asimismo acelerar la introducción de los servicios de acceso a Internet. En este contexto, la Comisión aprobó, el 24 de noviembre, una recomendación sobre la interconexión de líneas arrendadas, en la que entre otras cosas se insta a los Estados miembros a adoptar medidas (como el acceso desglosado de líneas arrendadas y la asignación de licencias a los bucles locales inalámbricos) que refuerzan la competencia para el acceso a la red local;
- extender el marco de normalización actual de las telecomunicaciones para abarcar todas las infraestructuras de comunicaciones y servicios asociados;
- proporcionar a los usuarios de telefonía móvil la selección del operador (forma de acceso a las redes obligatorias para las redes fijas en virtud del actual marco regulador sobre la interconexión), imponiendo ciertas obligaciones a los operadores de redes móviles con peso significativo en el mercado.

Gestión del espectro radioeléctrico

La existencia de una demanda considerable de utilización del espectro radioeléctrico en varios sectores, tales como las telecomunicaciones, el transporte, la seguridad pública, la radiodifusión y la I+D, pone de manifiesto la falta de eficacia de los métodos actuales de atribución de frecuencias y licencias. Dada la importancia del espectro radioeléctrico para el desarrollo de servicios de comunicaciones y en la medida en que la disponibilidad del espectro es limitada, la Comisión considera lo siguiente:

- la tarificación administrativa y la subasta de espectro radioeléctrico puede ser un modo de garantizar el uso eficiente del espectro;
- deben modificarse las disposiciones de la actual Directiva sobre licencias para permitir a los Estados miembros el comercio secundario con el espectro radioeléctrico como parte de un proceso para impulsar el uso eficiente del mismo.

Servicio universal

El marco regulador vigente exige a las ANR la imposición de obligaciones a los operadores de redes para garantizar que todos los ciudadanos tengan acceso a un conjunto mínimo definido de servicios de calidad específica que sea accesible a todos los usuarios con independencia de su situación geográfica y a un precio asequible. El servicio universal tal y como se define en la legislación comunitaria actual incluye la provisión de telefonía vocal y de fax y la transmisión a través de módems de datos en la banda vocal (es decir, acceso a Internet).

La Comisión reconoce la importancia del servicio universal y, entre otras cosas, propone lo siguiente:

- mantener en esta fase la definición y alcance actuales del servicio universal (proponiendo la definición de criterios para su eventual extensión y mecanismos de revisión periódica);
- poner a punto principios de tarificación a escala comunitaria para asegurar la asequibilidad del servicio universal.

Los intereses de usuarios y consumidores

El actual marco regulador contiene también cierto número de disposiciones dirigidas a proteger los intereses de los usuarios y consumidores en general. Además, existen a escala comunitaria diversas Directivas sobre la protección horizontal de los consumidores que son aplicables a todos los sectores, incluido el de las telecomunicaciones. En este sector, la Comisión propone lo siguiente:

- actualizar y aclarar la Directiva sobre datos personales para adaptarla al progreso tecnológico;

- hacer obligatoria la extensión del número europeo de llamada de urgencia (112);
- mantener y consolidar las obligaciones actuales en relación con la tramitación de denuncias y el arreglo de controversias;
- mejorar la transparencia de la información, incluida la relacionada con las tarifas, para los consumidores;
- exigir a los proveedores que faciliten a los consumidores información sobre la calidad del servicio;
- Derogar la Directiva 92/44/CE sobre líneas arrendadas tan pronto como exista la posibilidad de elección adecuada de líneas arrendadas para todos los usuarios y los precios de las mismas sean competitivos.

Numeración, nombres y direcciones

La legislación comunitaria actual define los elementos de la armonización en el ámbito de la numeración y de los nombres y las direcciones, y subraya la importancia de garantizar en toda Europa la interconexión de los usuarios de extremo a extremo y la interoperabilidad de los servicios. En este contexto, la Comisión propone lo siguiente:

- no adoptar medidas reguladoras por el momento en relación con los números y las direcciones Internet;
- extender la conservación del número a los usuarios móviles, pero por el momento no exigir la conservación del número entre las redes fijas y móviles.

Temas específicos de competencia

Las normas específicas del sector y la aplicación de las normas que regulan la competencia facilitan la entrada en un mercado en que los operadores históricos siguen detentando posiciones de fuerza y sirven para garantizar la competencia efectiva de los nuevos operadores. Por tanto, resulta fundamental encontrar el equilibrio adecuado entre una regulación específica del sector y las normas que regulan la competencia. En particular, convendría que la regulación específica del sector recurra más frecuentemente a conceptos propios del Derecho de la competencia, como el de posición dominante del artículo 82 del Tratado, en los casos, por ejemplo, de obligaciones con respecto a la orientación de los precios en función de los costes y la no discriminación.

Aspectos institucionales

El modelo regulador esbozado en la presente Comunicación implica reforzar la delegación de facultades de decisión en las ANR para garantizar que este marco se aplique lo más cerca posible del mercado en cada Estado miembro. Así, este modelo exige un mecanismo de contrapeso que refuerce la coordinación de las decisiones y posiciones de las ANR a escala de la Unión Europea.

En este contexto, la Comisión propone lo siguiente:

- sustituir los dos comités actuales en el ámbito de las telecomunicaciones por un nuevo Comité de las Comunicaciones que aproveche la experiencia de un nuevo Grupo de alto nivel sobre las comunicaciones integrado por las ANR y la Comisión para mejorar la aplicación coherente del Derecho comunitario y maximizar la aplicación uniforme de las medidas nacionales;
- revisar las disposiciones legales vigentes con vistas a reforzar la independencia de las ANR; garantizar un reparto eficaz de las responsabilidades entre las diferentes instituciones nacionales; mejorar la cooperación entre las autoridades específicas del sector y las autoridades nacionales en materia de competencia; exigir transparencia en los procedimientos de toma de decisiones a nivel nacional.

4) medidas de aplicación

Comunicación - COM(2000) 239 **final** Comunicación relativa a los resultados de la consulta pública sobre la Revisión de 1999 del sector de las comunicaciones y las orientaciones para el nuevo marco regulador.

De esta consulta se desprende que existe un amplio consenso sobre algunas propuestas y diferencias de opinión respecto de otras. En particular, la gran mayoría de los consultados apoyan las siguientes propuestas:

- mantener una reglamentación específica vigente en el sector paralelamente a la política de competencia, suprimiéndola cuando el mercado cumpla los objetivos;
- orientar a las autoridades nacionales de reglamentación (ANR) en las decisiones que deben tomar en su ámbito de competencia nacional para aplicar los objetivos normativos propuestos en la Comunicación;
- englobar todas las infraestructuras de comunicaciones y los servicios asociados;
- conseguir una mayor armonización de la normativa de los distintos Estados miembros;
- ampliar el principio de las autorizaciones generales para la prestación de servicios y redes de comunicaciones;
- asegurar una gestión más eficaz del espectro radioeléctrico y crear un grupo de expertos sobre política del espectro radioeléctrico;
- mantener el alcance actual de servicio universal;
- asegurar la posibilidad de desglosar los bucles locales en todos los Estados miembros;
- mantener el marco de normalización vigente;
- actualizar la Directiva vigente sobre protección de datos;
- retirar la Directiva sobre líneas arrendadas tan pronto exista una oferta competitiva suficiente de este tipo de líneas para todos los usuarios;
- establecer reglas encaminadas a definir mercados de manera dinámica en relación con las obligaciones de acceso e interconexión;
- adoptar medidas que garanticen la fuerza y la independencia de las ANR.

Aspectos en que existen diferencias de opinión:

- la financiación de las ANR por medio de los derechos de concesión de licencias;
- el procedimiento de venta del espectro y la posibilidad de que se admitan operaciones comerciales secundarias con el espectro radioeléctrico;
- la propuesta de introducción de dos umbrales para crear obligaciones asimétricas en cuestiones de acceso e interconexión (el peso significativo en el mercado y la posición dominante);
- las directrices para garantizar un servicio universal asequible;
- la portabilidad del número de teléfono para los usuarios de móviles;
- los mecanismos institucionales (divergencias de opinión sobre el papel del Comité de las Comunicaciones y el Grupo de Alto Nivel sobre las Comunicaciones);
- los ámbitos en los que siguen estando justificadas las autorizaciones específicas;
- los servicios ofrecidos a los usuarios (tales como la localización del llamante en las llamadas a servicios de urgencias y la transparencia de las tarifas por llamada)y calidad del servicio (intervención de las ANR en cuestiones de calidad del servicio).

Sobre la base de todos estos elementos, la Comisión ha de proponer, en junio de 2000, cinco directivas, en las que se incluyen una Directiva marco y cuatro Directivas específicas relativas al régimen de concesión de

licencias y autorizaciones, el acceso y la interconexión, los derechos de usuarios y consumidores en materia de servicio universal, y la protección de datos. Para elaborar estas propuestas, la Comisión se atendrá a las siguientes consideraciones básicas:

- las directrices establecidas en la Comunicación sobre la revisión del marco reglamentario;
- un amplio ámbito de aplicación que englobe todas las infraestructuras de comunicaciones y los servicios asociados;
- un sistema de concesión de autorizaciones generales;
- la modificación de la noción de "peso significativo en el mercado";
- la definición clara de los mercados que requieren la reglamentación ex ante;
- la protección de los intereses de consumidores y usuarios;
- la portabilidad del número de teléfono;
- la revisión de la Directiva sobre protección de datos personales;
- el acceso a la información sobre la localización del llamante en las llamadas a servicios de urgencias.

5) trabajos posteriores

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) [Diario Oficial L 201 de 31.7.2002].

Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco) [Diario Oficial L 108 de 24.4.2002].

Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización) [Diario Oficial L 108 de 24.4.2002].

Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal) [Diario Oficial L 108 de 24.4.2002].

Directiva 2002/19/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva acceso) [Diario Oficial L 108 de 24.4.2002].

Decisión 676/2002/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, sobre un marco regulador de la política del espectro radioeléctrico en la Comunidad Europea (Decisión espectro radioeléctrico) [Diario Oficial L 108 de 24.4.2002].

Última modificación: 02.12.2003

ANEXO 4

Convention on Cybercrime
CETS No.: 185

ture by the member States and the non-member States which have participated in its elaboration and for accession by other non States

Opening for signature

Place: Budapest
Date : 23/11/2001

Entry into force

Conditions: 5 Ratifications including at least 3 member States of the Council of Europe
Date : 1/7/2004

Status as of: 4/4/2014

Member States of the Council of Europe

	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/6/2002	1/7/2004				X			
Andorra	23/4/2013									
Armenia	23/11/2001	12/10/2006	1/2/2007				X			
Austria	23/11/2001	13/6/2012	1/10/2012		X	X	X			
Azerbaijan	30/6/2008	15/3/2010	1/7/2010		X	X	X	X		
Belgium	23/11/2001	20/8/2012	1/12/2012		X	X	X			
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006				X			
Bulgaria	23/11/2001	7/4/2005	1/8/2005		X	X	X			
Croatia	23/11/2001	17/10/2002	1/7/2004				X			
Cyprus	23/11/2001	19/1/2005	1/5/2005				X			
Czech Republic	9/2/2005	22/8/2013	1/12/2013		X	X	X			
Denmark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Estonia	23/11/2001	12/5/2003	1/7/2004				X			
Finland	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Georgia	1/4/2008	6/6/2012	1/10/2012			X				
Germany	23/11/2001	9/3/2009	1/7/2009		X	X	X			
Greece	23/11/2001									
Hungary	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Iceland	30/11/2001	29/1/2007	1/5/2007		X		X			

Ireland	28/2/2002									
Italy	23/11/2001	5/6/2008	1/10/2008				X			
Latvia	5/5/2004	14/2/2007	1/6/2007		X		X			
Liechtenstein	17/11/2008									
Lithuania	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003									
Malta	17/1/2002	12/4/2012	1/8/2012			X				
Moldova	23/11/2001	12/5/2009	1/9/2009			X	X	X		
Monaco	2/5/2013									
Montenegro	7/4/2005	3/3/2010	1/7/2010	55	X		X			
Netherlands	23/11/2001	16/11/2006	1/3/2007				X	X		
Norway	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Poland	23/11/2001									
Portugal	23/11/2001	24/3/2010	1/7/2010			X	X			
Romania	23/11/2001	12/5/2004	1/9/2004				X			
Russia										
San Marino										
Serbia	7/4/2005	14/4/2009	1/8/2009	55			X			
Slovakia	4/2/2005	8/1/2008	1/5/2008		X	X	X			
Slovenia	24/7/2002	8/9/2004	1/1/2005				X			
Spain	23/11/2001	3/6/2010	1/10/2010			X	X			
Sweden	23/11/2001									
Switzerland	23/11/2001	21/9/2011	1/1/2012		X	X	X			
The former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005				X			
Turkey	10/11/2010									
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			
United Kingdom	23/11/2001	25/5/2011	1/9/2011		X		X			

Non-members of the Council of Europe

	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Argentina										
Australia		30/11/2012 a	1/3/2013		X		X			
Canada	23/11/2001									

Chile										
Colombia										
Costa Rica										
Dominican Republic		7/2/2013 a	1/6/2013			X	X			
Israel										
Japan	23/11/2001	3/7/2012	1/11/2012		X	X	X			
Mauritius		15/11/2013 a	1/3/2014				X			
Mexico										
Morocco										
Panama		5/3/2014 a	1/7/2014				X			
Philippines										
Senegal										
South Africa	23/11/2001									
United States of America	23/11/2001	29/9/2006	1/1/2007		X	X	X			

Total number of signatures not followed by ratifications:	11
Total number of ratifications/accessions:	42

Notes:
(55) Date of signature by the state union of Serbia and Montenegro.
a: Accession - s: Signature without reservation as to ratification - su: Succession - r: Signature "ad referendum".
R.: Reservations - D.: Declarations - A.: Authorities - T.: Territorial Application - C.: Communication - O.: Objection.

ANEXO 5

eEurope 2002

1) OBJETIVO

Aumentar el número de conexiones a Internet en Europa, abrir el conjunto de las redes de comunicación a la competencia y estimular el uso de Internet haciendo hincapié en la formación y la protección de los consumidores.

2) ACTO

Comunicación de la Comisión, de 13 de marzo de 2001: «eEurope 2002 - Impacto y prioridades». Comunicación preparada para el Consejo Europeo de Estocolmo el 23 y 24 de marzo de 2001 [COM (2001) 140 final - sin publicar en el Diario Oficial].

3) SÍNTESIS

El plan de acción eEurope 2002 se inscribe directamente en el marco de la estrategia de Lisboa, pensada para convertir a la Unión Europea en la economía del conocimiento más dinámica y competitiva del mundo de aquí a 2010.

Las acciones se agruparon en torno a tres objetivos clave que debían alcanzarse para finales de 2002:

- una Internet más rápida, barata y segura;
- invertir en las personas y en la formación;
- estimular el uso de Internet.

Comunicación de la Comisión al Consejo y al Parlamento Europeo para el Consejo Europeo de Estocolmo del 23 y 24 de marzo de 2001 - eEurope 2002: Impacto y prioridades [COM (2001) 140 final - no publicada en el Diario Oficial].

Comunicación de la Comisión al Consejo y al Parlamento Europeo - Puesta al día sobre eEurope 2002, preparada por la Comisión Europea para el Consejo Europeo de Niza, 7 y 8 de diciembre de 2000 [COM (2000) 783 final - no publicada en el Diario Oficial].

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) [Diario Oficial L 201 de 31 de julio de 2002].

Reglamento (CE) n° 876/2002 del Consejo, de 21 de mayo de 2002, por el que se crea la Empresa Común Galileo [Diario Oficial L 138 de 28 de mayo de 2002].

Reglamento (CE) n° 733/2002 del Parlamento Europeo y del Consejo, de 22 de abril de 2002, relativo a la aplicación del dominio de primer nivel «.eu» [Diario Oficial L 113 de 30 de abril de 2002].

Comunicación de la Comisión, de 28 de mayo de 2002, al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones - eEurope 2005: Una sociedad de la información para todos - Plan de acción [COM(2002) 263 final - no publicada en el Diario Oficial];

Directiva 2002/38/CE del Consejo, de 7 de mayo de 2002, por la que se modifica y se modifica temporalmente la Directiva 77/388/CEE respecto del régimen del impuesto sobre el valor añadido aplicable a los servicios de radiodifusión y de televisión y a algunos servicios prestados por vía electrónica [Diario Oficial L 128 de 15 de mayo de 2002].

Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco) [Diario Oficial L 108 de 24 de abril de 2002].

Directiva 2002/19/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva acceso) [Diario Oficial L 108 de 24 de abril de 2002].

Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización) [Diario Oficial L 108 de 24 de abril de 2002].

Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal) [Diario Oficial L 108 de 24 de abril de 2002].

Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones de 26 de enero de 2001 - Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos - eEurope 2002 [COM (2000) 890 final - no publicada en el Diario Oficial].

Decisión 2001/48/ CE del Consejo, de 22 de diciembre de 2000, por la que se adopta un programa plurianual comunitario de estímulo al desarrollo y el uso de contenidos digitales europeos en las redes mundiales y de fomento de la diversidad lingüística en la sociedad de la información [Diario Oficial L 14 de 18 de enero de 2001].

Reglamento (CE) nº 2887/2000 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, sobre el acceso desagregado al bucle local [Diario Oficial L 336 de 30 de diciembre de 2000].

Última modificación: 25.04.2003

ANEXO 6

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 11.2.2003
COM(2003) 66 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

eEurope 2002 Final Report

Nota:
De este anexo solo retomé la introducción y las conclusiones del Reporte Final porque es lo más relevante. Nos dirá el propósito de este ejercicio y lo que se obtuvo a partir de los ejercicios realizados en el eEurope 2002.

INTRODUCTION

The *e*Europe 2002 Action Plan was endorsed at the Feira European Council in June 2000 as part of the decade-long Lisbon strategy of economic, social and environmental renewal. It was complemented by the *e*Europe+ initiative launched by the candidate countries in reply to the invitation of the Feira European Council to take on board the Lisbon strategy. The Action Plan set out 11 action areas in which there were a total of 64 targets to be achieved before the end of 2002.

*e*Europe targets have been monitored regularly through the benchmarking exercise. Benchmarking forms part of the open method of co-ordination, promoted by the Lisbon European Council, whereby monitoring, exchange of best practices and peer review are applied to improve convergence of national performances towards the goals and targets for the Union set out in the Lisbon strategy. The benchmarking of *e*Europe is based on a list of 23 sector-specific indicators endorsed by the Council in November 2000. Intermediate measurements of these indicators were presented in the Commission Communications '*Impacts and Priorities*' in March 2001[1] and '*eEurope Benchmarking Report*' of February 2002[2].

The present document highlights the achievements of *e*Europe and identifies remaining obstacles to the full development of the information society in Europe. There is also an accompanying [Commission Staff Working Paper] which provides a commentary on progress in each of the 64 targets.

---

[36] *e*Europe 2005 Action Plan, COM(2002) 263.

In terms of realising the targets endorsed at the Feira European Council, *e*Europe has been a major success. Most of the 64 targets have been achieved. Its success is due to the contributions of many actors in the European Institutions, Member States, Industry and Social Partners. Its achievements are notable as they have been realised despite the difficulties of a sharp decline in the stock market, particularly in ICT stocks, high levels of debt, and subsequent reductions in investment. The goal of a competitive knowledge based economy is still some distance away, but *e*Europe has laid solid foundations.

In general *e*Europe has been strong on bringing citizens and businesses online and establishing a framework within which the knowledge economy can grow. Translating these achievements into tangible economic benefits, higher productivity, improved quality of service, greater social inclusion and non-inflationary growth, cannot be done quickly. Achieving these gains through effective use can only be realised by restructuring economic behaviour, modernising practices and undergoing organisational change to exploit the new technologies. This is a long run process and achieving it in two years was beyond the scope of *e*Europe 2002. To summarise:

- **Internet connectivity has grown rapidly**. When *e*Europe was launched, few had access to the Internet. In 2002, more than 90% of schools and businesses are online and more than half of Europeans are regular users. Europe now has the fastest backbone research network in the world. Widespread take up of high-speed connections by households and SMEs is going to be the next challenge. There are still significant differences in connectivity between Member States.

- A **legislative framework** for **electronic communications** and for **e-commerce** has been agreed. Telecom legislation has been designed to strengthen competition in the market and thereby reduce prices and to stimulate innovation. Prices have fallen and that competition has been improving. For e-commerce, a series of directives have been adopted to increase certainty in e-commerce transactions, in particular cross-border trade, and to ensure an adequate level of consumer protection.

- **Increasing effective use of the Internet** is the focus of the next step, eEurope 2005. This means for example, more firms to use e-commerce; schools not only connected but also making full use of the Internet in class; government services offered online as well as fully interactive, more use in the health sector where there are great demands for up-to-date information. More training is needed for the benefit both of workers and companies. Action must be taken to address the current gaps in access and use of digital technologies so to ensure that all Europeans have the opportunity to take advantage of them for their social and working life.

A detailed analysis of the benchmarking statistics that led to these conclusions is given in section 2. This is followed by Conclusions focusing on the removal of residual obstacles to the full development of the digital economy.

CONCLUSIONS

This evaluation has shown that *e*Europe 2002 achieved its main objectives and that these represent important steps towards the knowledge-based economy which is at the centre of the Lisbon strategy.

As access prices have fallen, the number of households connected to the Internet in Europe has risen to over 40%. More than 90% of schools and 90% of businesses are nowadays connected. With Géant, Europe now has the world's fastest backbone research network connecting nearly all universities and research institutes and representing a test-bed for future Internet technologies. Development of competition is likely to further drive down prices, in particular for broadband access, to increase innovation and broaden the range of services.

Moreover, new services and the Internet have opened up new opportunities for society as a whole, helped by the creation of a comprehensive legal framework in e-commerce, and will be further stimulated by the upcoming transposition and implementation of the new regulatory framework for electronic communications. There is an increasing number and higher quality of e-government services becoming available online across the whole of Europe.

The upward trend in the use of information and communication technologies and services (ICTs) in the economy and society is very encouraging. The starting point is now better than ever for Europe to draw the full benefits of digital technologies and the Internet in terms of productivity gains, economic growth, employment and social cohesion. Yet conditions ought to be even better, in particular with regard to the existing gaps in Internet use among the different groups and to the use of ICT and e-business by European SMEs. Therefore, Europe ought to realise the efficiencies and opportunities intrinsic to the adoption of these technologies.

Basic e-government services are online. Now they need an increasing degree of interactivity and require back-office reorganisation to fully achieve efficiencies. Most schools are now connected. The next step is to use computers more effectively to improve education and skills. The work of medical practitioners at all levels is becoming more information intensive. The development of health information networks with broadband connectivity is becoming a critical infrastructure for the provision of health services. Much work has been done to improve the security of information infrastructures by both the private and public sector but threats remain and the consequence of attacks are increasingly costly. It is essential for security work to continue and a centre of competence be established to stimulate e-commerce and Internet use in general. Internet connections have greatly improved, obviously initially mainly narrowband. Europe must now move broadband; a leading-edge infrastructure being a prerequisite for a competitive knowledge economy. In general, the pervasive use of ICTs across a wide range of economic and social activities supported by broadband networks can bring about a profound and long-term impact on productivity growth and *e*Europe 2002 has initiated this process.

The next stage in the development of the information society and its contribution to the Lisbon objectives is already underway in the form of the *e*Europe2005 Action Plan[36] which covers the period 2003-2005. The objectives of the new Action Plan were endorsed by Heads of State and Government at Seville in June 2002 and is already providing an effective response to many of the issues highlighted in this Report.

The new Action Plan focuses on a more limited number of key targets where government action can make a genuine difference: the modernisation of public services to make them more productive, accessible and equitable; the further promotion of a favourable environment for e-business; and a secure broadband information infrastructure. Cutting across these priorities is the necessity to create an inclusive information society for all of Europe's citizens.

The extensive use of a wide range of different ICT applications, content and services, both by the public and private sectors, is expected to improve productivity and competitiveness in the EU economy as a whole, creating a favourable environment to private investment, and making an important contribution to meeting the Lisbon agenda.

---

[36] *e*Europe 2005 Action Plan, COM(2002) 263.

ANEXO 7

i2010: la sociedad de la información y los medios de comunicación al servicio del crecimiento y el empleo

i2010 es el nuevo marco estratégico de la Comisión Europea por el que se determinan las orientaciones políticas generales de la sociedad de la información y los medios de comunicación. Esta nueva política integrada se propone, en particular, fomentar el conocimiento y la innovación al objeto de promover el crecimiento y la creación de empleo, tanto cualitativa como cuantitativamente. Se inscribe en el marco de la revisión de la Estrategia de Lisboa.

ACTO

Comunicación de la Comisión, de 1 de junio de 2005, al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones titulada «i2010 - Una sociedad de la información europea para el crecimiento y el empleo» [COM(2005) 229 final - No publicada en el Diario Oficial].

SÍNTESIS

Con i2010, la Comisión aborda de manera integrada la sociedad de la información y las políticas audiovisuales en la Unión Europea. Su propósito es coordinar la acción de los Estados miembros para facilitar la convergencia digital y afrontar los desafíos vinculados a la sociedad de la información. Para elaborar este marco estratégico, la Comisión ha llevado a cabo una amplia consulta con las partes interesadas en torno a iniciativas e instrumentos anteriores, tales como e-Europa y la Comunicación sobre el futuro de la política reglamentaria europea en el ámbito audiovisual.

La Comisión propone tres prioridades que se deben alcanzar antes de 2010 para las políticas europeas de la sociedad de la información y los medios de comunicación: la consecución de un espacio europeo único de la información; el impulso de la innovación y de la inversión en el campo de la investigación en las tecnologías de la información y la comunicación (TIC), y la consecución de una sociedad de la información y los medios de comunicación basada en la inclusión.

Un espacio europeo único de la información

Con el fin de lograr un mercado interior abierto y competitivo para la sociedad de la información y los medios de comunicación, el primer objetivo de i2010 es el de establecer un Espacio Único Europeo de la Información que ofrezca comunicaciones de banda ancha asequibles y seguras, contenidos ricos y diversificados y servicios digitales. La Comisión se propone alcanzar cuatro grandes metas:

- aumentar la velocidad de los servicios de banda ancha en Europa;
- fomentar los nuevos servicios y los contenidos en línea;
- potenciar los dispositivos y las plataformas capaces de «hablar entre sí»;
- hacer que Internet sea más segura frente al fraude, los contenidos nocivos y los fallos tecnológicos.

Para la realización del Espacio Único Europeo de la Información, la Comisión tiene la intención de:

- revisar el marco reglamentario de las comunicaciones electrónicas, incluida la determinación de una estrategia eficaz de gestión del espectro radioeléctrico;
- crear un marco coherente para los servicios de la sociedad de la información y los medios de comunicación mediante:
  - la modernización del marco jurídico de los servicios audiovisuales, comenzando por la revisión de la Directiva «Televisión sin fronteras» (2005);
  - las modificaciones necesarias en los elementos del acervo comunitario que tengan una incidencia en los servicios de la sociedad de la información y los medios de comunicación (2007);
  - la promoción activa de la aplicación rápida y eficiente del acervo existente y actualizado;
- dar un apoyo permanente a la creación y circulación de contenidos europeos, por ejemplo a través de los programas «eLearning» y «eContentplus», y sus sucesores;
- establecer una estrategia en favor de una sociedad de la información segura, que incluirá la sensibilización sobre la necesidad de autoprotección, la vigilancia y el seguimiento de las amenazas y la respuesta rápida y eficaz a los ataques y a los fallos del sistema;
- definir y promover acciones centradas en la cuestión de la interoperabilidad, en particular la gestión de derechos digitales.

Innovación e inversión en investigación

Con el fin de impulsar la innovación y la inversión en la investigación de las TIC, la Comisión desea situar el rendimiento de la investigación y la innovación en TIC en un alto nivel mundial, reduciendo así la distancia que separa a Europa de sus principales competidores, y propone:

- aumentar en un 80% el apoyo comunitario a la investigación sobre TIC para el año 2010 e invitar a los Estados miembros a hacer lo propio;
- dar prioridad a los pilares tecnológicos clave del 7º Programa Marco de Investigación y Desarrollo tecnológico (PMID), a saber, las tecnologías del conocimiento, los contenidos y la creatividad, las redes de comunicación avanzadas y abiertas, el software seguro y fiable, los sistemas integrados y la nanoelectrónica;
- poner en marcha iniciativas de investigación y despliegue que permitan resolver los obstáculos esenciales en materia de interoperabilidad, seguridad y fiabilidad, gestión de identidades y gestión de derechos, que exigen soluciones tanto tecnológicas como organizativas;
- determinar medidas complementarias de fomento de la inversión privada en investigación e innovación en el ámbito de las TIC (2006);
- formular propuestas especificas sobre una sociedad de la información para todos en las orientaciones estratégicas comunitarias en materia de cohesión para el periodo 2007-2013;
- definir políticas de comercio electrónico encaminadas a suprimir los obstáculos tecnológicos, organizativos y jurídicos que dificultan la adopción de las TIC, haciendo especial hincapié en las pequeñas y medianas empresas (PYME);
- desarrollar herramientas de apoyo a los nuevos patrones de trabajo, herramientas que potencian la innovación en las empresas y la adaptación a las nuevas necesidades de capacitación.

Inclusión, mejora de los servicios públicos y de la calidad de vida

G

La Comisión desea reforzar la cohesión social, económica y territorial merced a la consecución de una sociedad europea de la información basada en la inclusión. Desea fomentar el crecimiento y el empleo de una manera coherente con el desarrollo sostenible y dar prioridad a la mejora de los servicios públicos y de la calidad de vida. Para lograr el objetivo de una sociedad de la información que sea incluyente, ofrezca servicios públicos de gran calidad y promueva la calidad de vida, la Comisión propone, entre otras cosas:

- publicar unas orientaciones políticas sobre accesibilidad electrónica y cobertura territorial de la banda ancha con el fin de facilitar la utilización de los sistemas TIC por un mayor número de personas (2005);
- proponer una iniciativa europea sobre inclusión electrónica (e-inclusión) que aborde la igualdad de oportunidades, las competencias en TIC y las fracturas regionales (2008);
- adoptar un plan de acción sobre administración electrónica y orientaciones estratégicas para estimular el uso de las TIC en los servicios públicos; pondrá en marcha proyectos de demostración para someter a prueba, a escala operativa, soluciones tecnológicas, jurídicas y organizativas que permitan ofrecer servicios públicos en línea;
- poner en marcha, en un primer momento, tres iniciativas pioneras que implican el uso de TIC a fin de mejorar la calidad de vida: servicios de atención a las personas en una sociedad que envejece, unos transportes más seguros y menos contaminantes, en particular «automóvil inteligente», y bibliotecas digitales para promover la diversidad cultural.

Gobernanza

La Comisión tiene la intención de elaborar propuestas de actualización de los marcos reguladores de las comunicaciones electrónicas y de los servicios de la sociedad de la información y los medios de comunicación. Se propone también utilizar los instrumentos financieros comunitarios para estimular la inversión en investigación estratégica y para suprimir los obstáculos que dificultan la innovación en el ámbito de las TIC. Finalmente, desea fomentar las políticas que aborden la inclusión digital y la calidad de vida.

En el marco de los programas nacionales de reforma, los Estados miembros se comprometieron a adoptar para mediados de octubre de 2005 las prioridades referidas a la sociedad de la información en consonancia con las directrices integradas para el crecimiento y el empleo. En particular, procurarán:

- incorporar a su ordenamiento de forma rápida y completa los nuevos marcos reguladores que afectan a la convergencia digital, haciendo hincapié en mercados abiertos y competitivos;
- aumentar la parte del gasto nacional dedicada a la investigación sobre TIC con el fin de desarrollar servicios públicos modernos e interoperables basados en las TIC;
- fomentar la innovación en el sector de las TIC merced a la inversión;
- fijar objetivos ambiciosos para la evolución de la sociedad de la información a nivel nacional.

Los Estados miembros han presentado sus realizaciones en el marco determinado con motivo de la revisión de la Estrategia de Lisboa.

La Comisión invita igualmente a las demás partes interesadas a que emprendan un diálogo abierto y constructivo en apoyo de la sociedad de la información. Se dirige, en particular, a los socios industriales para que aumenten la inversión en la investigación y las tecnologías de este ámbito.

Con el fin de reunir a todas las partes interesadas, la Comisión propone que se utilice el método abierto de coordinación, que combina el intercambio de buenas prácticas con la elaboración de informes anuales acerca de la puesta en práctica de los objetivos de Lisboa.

ACTOS CONEXOS

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Informe sobre la competitividad digital de Europa: principales logros de la estrategia i2010 entre 2005 y 2009 [COM(2009) 390 final – no publicada en el Diario Oficial]

La presente Comunicación hace balance de la estrategia «i2010» llevada a cabo entre 2005 y 2009. En ella se concluye que las acciones emprendidas en materia de TIC a lo largo de estos cuatro años han modernizado Europa desde el punto de vista económico y social, y han contribuido al logro de estos resultados:

- el número de europeos en línea se ha incrementado en gran medida, sobre todo entre los grupos desfavorecidos;
- Europa se ha convertido en líder mundial de la Internet de banda ancha;
- las conexiones de banda ancha han aumentado;
- Europa es líder mundial en telefonía móvil;
- la oferta y la utilización de servicios en línea se ha incrementado de manera considerable;
- se han realizado importantes avances en el sector de las TIC asociados a la microelectrónica, la nanoelectrónica, en la atención sanitaria y en el programa de seguridad vial;
- las políticas en el ámbito de las TIC se han integrado cada vez más en las demás políticas.

No obstante, la Unión Europea aún presenta un retraso notable en el ámbito de la investigación y el desarrollo de las TIC con respecto a Estados Unidos, Japón o Corea del Sur. Por lo tanto, para mantener su competitividad, es importante que Europa cuente con una nueva agenda digital. Para ello, la Comisión quiere realizar una consulta pública en línea sobre algunos aspectos clave para las futuras políticas de la UE en el ámbito de las TIC y los medios de comunicación.

Comunicación de la Comisión, de 17 de abril de 2008, al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Preparar el futuro digital de Europa – Revisión intermedia de la iniciativa i2010 [COM(2008) 199 final - No publicada en el Diario Oficial]. La Comisión observa un gran crecimiento de la banda ancha en Europa. Más de la mitad de los europeos (250 millones de personas) utiliza regularmente Internet. En 2007 se sumaron casi 40 millones de nuevos usuarios. Los servicios públicos —el 96% de las escuelas europeas y el 57% de los médicos, recurren cada vez más a las conexiones de banda ancha. En cuanto a las empresas, el 77% dispone de una conexión de banda ancha. El acceso de banda ancha se está convirtiendo gradualmente en el tipo de conexión habitual.

Con todo, además de señalar el gran crecimiento de la banda ancha en la UE, este informe formula también una serie propuestas concretas para reorientar la iniciativa i2010 en el periodo 2008-2010. El objetivo consiste en promover la competitividad de los países más avanzados al tiempo que se reducen las distancias entre los Estados miembros. En concreto, la Comisión quiere impulsar las iniciativas tecnológicas comunes para favorecer la investigación en el campo de las TIC. En 2008 se publicará una guía de los derechos y obligaciones de los usuarios de las técnicas digitales en la UE a fin de fomentar el uso de las nuevas tecnologías en línea y reducir la brecha digital entre los Estados miembros. Asimismo, la Comisión tiene previsto desarrollar servicios públicos paneuropeos, tales como las iniciativas relativas a la identidad y firma electrónicas.

Comunicación de la Comisión, de 30 de marzo de 2007, al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: i2010 – Informe anual sobre la sociedad de la información 2007 [COM(2007) 146 final – No publicada en el Diario Oficial].

En este segundo informe, la Comisión formula las siguientes recomendaciones y actuaciones para 2007 y 2008:

- revisión del marco reglamentario de las comunicaciones electrónicas;
- prosecución de la política de innovación de las TIC mediante iniciativas tecnológicas conjuntas, la política de normalización de la UE o el Programa Marco para la Innovación y la Competitividad (PIC);
- inclusión y mejora permanente de los servicios públicos y de la calidad de vida (accesibilidad electrónica, alfabetización digital, administración en línea, automóvil inteligente y eficiencia energética).

Con vistas a un examen intermedio en 2008, el informe define las siguientes actuaciones preparatorias:

- definición de las perspectivas de evolución, en particular a través de las posibilidades de la nueva Internet, en colaboración con el Grupo de Alto Nivel i2010;
- realización de una consulta pública multipartita;
- planteamiento de los grandes temas del examen intermedio en un acto i2010 de alto nivel en 2008.

El fruto de estos intercambios alimentará en parte los debates del Consejo Europeo de la primavera de 2008, en el que se estudiarán los problemas de la Internet de nueva generación.

Última modificación: 09.12.2009

Fuentes de Consulta

Libros

- Assange, Julian (2015). *Cypherpunks*. Temas de hoy. México-Estados gUnidos. Editorial Planeta. p. 345
- Batta Fonseca, Víctor (2010). *Prospectiva y Teoría Internacional: Escenarios sobre el Estado y la Gobernabilidad en el siglo XXI*. UNAM, México. p. 345
- Carr Jeffrey (2010). *Inside Cyber Warfare*. O'Reilly, Estados Unidos, California, p. 156
- Clarke, Richard A. (2015). *Guerra en la red: los nuevos campos de batalla*. Ariel, España, p. 369
- Dodge Martin (2001). *Atlas of cyberspace*. Pearson Education Ltd, Inglaterra, p. 506
- E. Reyes, Giovanni. *Teoría de la globalización: Bases fundamentales*. Siglo XXI. México. p. 113
- Ganuza Artiles, Nestor (2014). *La situación de la ciberseguridad en el ámbito internacional y en la OTAN*. Cuadernos de estrategia en Ciberseguridad: Retos y amenazas de la Seguridad Nacional en el ciberespacio; España, p. 345
- Ibáñez, Josep, *Globalización e Internet: poder y gobernanza en la sociedad de la información*, en Batta Fonseca, Víctor; Prospectiva y Teoría Internacional: Escenarios sobre el Estado y la Gobernabilidad en el siglo XXI, UNAM, México, p. 325
- Lessig, Laerence (2009). *El Código 2.0*. Traficantes de sueños, Madrid, España, p. 545
- Manuel Castells (2000). *The Information Age: Economy, Society and Culture*. Volume I: The Rise of the Network Society, Oxford, Blackwell, 2nd, p.289
- Misseri, Lucas (2015). *Ciberespacio y praxis: algunas reflexiones ético-politicas*. Kazak Ediciones, Argentina, p. 356

- Sánchez Medero, Gema (2010). *Los Estados y la ciberguerra*. Universidad Complutense de Madrid, España. p. 63-75
- Secretaría de Marina Armada (2015). *Seguridad y Defensa en el Ciberespacio*, Centro Superior de Estudios Navales. México, p.507

Documentos oficiales

- Comisión de las Comunidades Europeas (2004). *Comunicación de la Comisión al Consejo y al Parlamento Europeo: Prevención, preparación y respuesta a los ataques terroristas*. Bruselas. 30 p.
- Comisión de las Comunidades Europeas (2005). *Libro Verde sobre un programa europeo para la protección de infraestructuras críticas.* Bruselas. 105 p.
- Comisión Europea (2001). *Seguridad de las Redes de Información: Propuesta para un enfoque político europeo*; Unión Europea; Comité de las Regiones, 30 p.
- Comisión Europea (2013). *Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro*. Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad; Bruselas, 30 p.
- Comisión Europea (2014). *Agenda Digital para Europa: Comprender la políticas de la Unión Europea*, Bruselas, Bélgica, 12 p.
- Consejo Europeo (2001). *Convenio de Budapest sobre la ciberdelincuencia.* Budapest; 70 p.
- Secretaría del Consejo de la Unión Europea (2009). *Estrategia Europea de Seguridad*. Consejo de la Unión Europea. Bruselas; p.15

Artículos Espacializado

- Ángel Pérez González (2001). Minorías rusas en la antigua URSS. *Afers Internacionals*. (No. 52) p. 51

- Bryant, Rebecca (2001), What Kind of Space is Cyberspace? *An Internet Journal of Philosophy*, Vol. 5, p. 19
- Buzai, Gustavo (2012). El Ciberespacio desde la Geografía. Nuevos espacios de vigilancia y control global. *Revista de Geografía Meridiano*. (No. 1) p. 14
- Cabeza Morillo, Hilda (2015). Territorio y espacio geográfico. *Revista de Facultad de Ciencias Jurídicas y Políticas de la Universidad de los Andes*. Vol. 3, p. 12
- Eissa, Sergio Gabriel (2014). El Ciberespacio y sus implicancias para la defensa nacional. Aproximaciones al caso argentino. *Revista de Ciencias Sociales, segunda época*. (Nº 25). pp. 275
- Fundación CIDOB. Los Conflictos de la Federación Rusa. *CIDOB*. (No. 26). p. 15
- García, Javier (2016). La Unión Europea y la OTAN en el marco de la Nueva Estrategia Global de la Unión Europea. *Revista UNISCI*. (No. 42). España, p. 23
- Gazapo, Manuel (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista UNISCI*. (No. 43). Madrid.p.86
- Hernán Gómez de Mateo, José Luis (2014); Dilemas Cibernéticos y la Estrategia de Seguridad Nacional; *Instituto Español de Estudios Estratégicos*; España; p. 5
- Hughes, Rex (2010); A treaty for cyberspace; *Revista Royal Institute of International Affairs*; Vol. 86, pp. 523-541
- Izquierdo, José de Carlos (30 de septiembre de 2016). La nueva Estrategia de Seguridad Europea 2016. *Instituto Español de Estudios Estratégicos*. España, p. 40
- Laborie Iglesias Mario (2016). Hacia unas nuevas (e impredecibles) relaciones OTAN-UE. *Revista Española de Defensa*. España; p. 67
- Margarita Rohr Trushchelevea (2014). La evolución de demográfica y la importancia de flujos migratorios en Rusia: un recorrido histórico. *Universidad de Valencia*. Vol. 21. (No. 86). p. 30
- Ministerio de defensa (2011). Nuevo concepto de ciberdefensa de la OTAN. *Instituto Español de Estudios Estratégicos*. (No. 9). p. 34

- Ministerio de Defensa (2012). El Ciberespacio. Nuevo escenario de confrontación. *Monografías del Centro de Estudios de la Defensa Nacional (CESEDEN).* España. P. 21
- Molina Mateos, José María (2014); Globalización, Ciberespacio y Estrategia Especial Consideración a la Estrategia de la Información. *Instituto Español de Estudios Estratégicos*. España. p.25
- Ramírez Morán, David (2015). La visión internacional de la ciberseguridad. *Revista del Instituto Español de Estudios Estratégicos.* España. p. 1-9
- Realpe Díaz, Milena Elizabeth (2016). *La ciberguerra, una amenaza a la Seguridad y Defensa Nacional. Centro Superior de Estudios Navales (Ed.), Seguridad y Defensa en el Ciberespacio.* México, p. 456
- Rodríguez Suárez, Pedro Manuel (Marzo 2015). Los países bálticos frente a Europa y Rusia. *Revista de la Facultad de Derecho y Ciencias Sociales*. (No. 37). México, p.19
- Sain, Gustavo. ¿Qué es la ciberguerra? *Revista Pensamiento Penal (*No. 10). España. p. 12
- Sánchez Medero, Gema (2011). La ciberguerra: los casos de Stuxnet y Anonymus. *Nueva Época*. (No. 11). España. p. 250
- Stephen Herzog (2011). Revisting the Estonian Cyber Attacks: Digital Threats and Multinational Respons. *Journal of Strategic Security*. (No. 2), p. 60
- Uruena, Francisco (2015). Amenaza de los ciberataques. *Instituto Español de Estudios Estratégicos*. España. p. 15

Artículos especializados en línea

- A.A.K (3 julio de 2013). How did Estonia become a leader in technology? *Way Back Machine* Recuperado en: https://goo.gl/24rdzq
- ABADAL, Ernest (2011). Agenda digital europea: las cosas que se deben hacer para mejorar en TIC en Europa. *Blok de bid*. Recuperado en: http://goo.gl/dW6dlH

- Arteaga, Felix (2015). La Estrategia Europea de Seguridad, cinco años después. *Real Instituto El Cano Royal Institute*. España, Recuperado en: http://bit.ly/2nHUwPr
- Barlow, John P. (1998). A Declaration of the Independence of Cyberspace. Recuperado en: https://goo.gl/JKZh6D
- Domínguez Cebrian, Belén (28 de Marzo de 2017). Dinamarca abre embajada en Silicon Valley. *El País*. Madrid, España. Recuperado en: https://goo.gl/A4HBuL
- Editorial (2014). Estas son las 10 ciberamenazas más comunes. *Periódico ABC*. Recuperado en: https://goo.gl/PJzGEi
- Editorial (2015), Historia de Internet. UPC. Recuperado en: https://goo.gl/zrps8X
- Ernest Abadal (2011), "Agenda digital europea: las cosas que se deben hacer para mejorar en TIC en Europa", Blok de bid, Recuperado en: http://goo.gl/dW6dIH
- Estonia Goberment (2001-2017). e-estonia. Tallin, Estonia. Recuperado en: https://e-estonia.com/#
- Freet, Nahun (2015). ¿Qué es un ciberataque? Auditool. España, Recuperado en: https://goo.gl/CxZ3hs
- Gallagher, Sean (2015). Cybergeddon: Why the Internet could be the next "failed state". ARS Technica. Recuperado en: https://goo.gl/U5cfML
- GEDEON (1 de junio de 2013) "Ciberguerrilla", GEDEON, Recuperado en: https://goo.gl/Xbs3mu
- Gómez Arriagada, Héctor (2013). Ciberoperaciones. REVISMAR. Recuperado en: https://goo.gl/4gBLUm
- Guillermo Julian (2 de febrero de 2012), "¿Son los DDoS efectivos como medios de protesta?", GENBETA, Recuperado en: http://goo.gl/uwrdOh
- Hernández, Adolfo; Estrategias nacionales de ciberseguridad en el mundo; Red de Seguridad; Recuperado en: https://goo.gl/r8EGu1
- Jornadas de Ciberdefensa 2016 Mando Conjunto de Ciberdefensa. Recuperado en: https://goo.gl/rpehcr
- José Ángel Martos (9 de noviembre de 2014), ¡Esto es la Ciberguerra!, Muy Interesante, Recuperado en: http://goo.gl/DFowA6

- JULIAN, Guillermo (2 de febrero de 2012), “¿Son los DDoS efectivos como medios de protesta?”, *GENBETA,* Recuperado en: http://goo.gl/uwrdOh
- Laborie Iglesias, Mario A. (2010); La cooperación OTAN-UE en el futuro concepto estratégico de la Alianza Atlántica;Real Instituto Elcano; Recuperado en: https://goo.gl/qGvNGu
- Losa, Guillermo, “¿Qué tienen en común Netflix, Uber y Airbnb?”, El Observador, Recuperado en: https://goo.gl/XuTVYg
- MARTÍNEZ DE RITUERTO, Ricardo (7 de mayo de 2008), “El militar de bronce que divide Estonia”, *El País,* Recuperado en: http://goo.gl/5uHiJF
- MARTOS, José Ángel (9 de noviembre de 2014), “¡Esto es la Ciberguerra!”, *Muy Interesante*, Recuperado en: http://goo.gl/DFowA6
- Navarro, Beatriz (4 de Julio de 2017), Estonia abre la primera embajada digital para proteger sus datos, Tallin, Estonia. Recuperado de: https://goo.gl/LZZhBT Coello, Claudio (2017), La Europa Digital: competitividad, progreso e integración, Comisión Europea. Recuperado de: https://goo.gl/WMqyRm
- Ortiz, Carlos (2006). La Política europea en materia de telecomunicaciones: hacia la nueva sociedad de la información. Noticias Jurídicas. Recuperado de: https://goo.gl/5CNPYP
- OTAN (2007), Tallinn Manual: Panel of Experts, Cooperative Cyber Defense of Excellence, Recuperado de: https://goo.gl/rR3SSm
- Pérez Porto, Julian (2011), Espacio Geográfico, Recuperado en: https://goo.gl/C6McZy
- RIA Novosti (9 de mayo de 2007), Putin: “El 9 de mayo es una fiesta de enorme trascendencia moral”, Sputnik News. Recuperado en: https://sptnkne.ws/g4G2
- Ricardo Martínez de Rituerto (7 de mayo de 2008), “El militar de bronce que divide Estonia”, El País. Recuperado en: http://goo.gl/5uHiJF
- Robles Carrillo, Margarita (2016), Uso de la fuerza en el ciberespacio: las armas cibernéticas. Jornadas de Ciberdefensa 2016 Mando Conjunto de Ciberdefensa. Recuperado en: https://goo.gl/rpehcr

- Rodríguez U., Migue Luis (2011, 7 de mayo), Poder Virtual como espacio geopolítico, Geopolítica XXI. Recuperado en: https://goo.gl/i3ypgG
- RUIZ, Francisco J. (7 de noviembre de 2013), “El problema de los no ciudadanos en las repúblicas bálticas”*, Russia Beyond The Headlines,* Recuperado de: https://goo.gl/wrkYjR
- Sturm, Cony (2013). Operación Octubre Rojo: Es un nuevo ataque contra diplomáticos y organizaciones gubernamentales. Fayer Wayer. Recuperado de: https://goo.gl/ELSQkL
- Vázquez Ortiz, Ana Pilar (2016), Principios del Derecho Internacional aplicables a la acción de los Estados en el ciberespacio. Jornadas de Ciberdefensa 2016 Mando Conjunto de Ciberdefensa. Recuperado de: https://goo.gl/rpehcr

Páginas Especializadas

- Comisión Europea (2001). eEurope 2002: Impacto y prioridades. *Comisión Europea*. Recuperado en: https://goo.gl/wrcL1q
- Comisión Europea (2015). Estrategia Europa 2020. *Gobernanza Económica de la Unión Europea*. Recuperado en: https://goo.gl/gP9pgf
- Comisión Europea (2017). La UE y el Mercado Único Digital. *Unión Europea.* Recuperado en: https://goo.gl/PzKC2o
- Comité Internacional de la Cruz Roja (2010). Jus ad bellum y Jus in bello. *CICR*. Recuperado en: https://goo.gl/W8YdDL
- Computación Aplicada al Desarrollo S. A. (2015). Historia de Internet. *CAD*. Recuperado en: https://goo.gl/U3w47P
- Conde, Rubén (2017). Los Ciberataques: tipos y previsiones para 2018. *RCG Comunicaciones*. Recuperado en: https://goo.gl/nzFCMc
- Consejo Europeo (2016), Cooperación de la UE en materia de seguridad y defensa. *Unión Europea.* Recuperado en: https://goo.gl/Bj8nNR
- DCAF (2009), Democratic Gobernance Challenge of Cyber Security. *DCAF*. Recuperado en: https://goo.gl/C6SDzD
- DI PACE, Damián. El Milagro de Estonia, la improbable meca

tecnológica de Europa. *Infobae*. Recuperado en: http://goo.gl/a6xOrt

- Editor (2010) ¿Qué es el Ciberespacio? *Interflicto.com* Recuperado en: https://goo.gl/wwvwx3
- Editorial (2012), Funcionamiento del ISP. *Manurevah*. Recuperado en: https://goo.gl/TQGGjW
- Editorial (2016). ¿Qué es Blockchain, la tecnología que viene a revolucionar las finanzas? *INFOTECHNOLOGY*. Recuperado en: https://goo.gl/7ZRMiu
- ENISA (2015). Conclusion for the European Public-Private Partnership (PPP) for Resilience scheme. *Unión Europea.* Recuperado en: https://goo.gl/fst3Qw
- ENISA (2018). Visión General. *Unión Europea*. Recuperado en: https://goo.gl/pP3oeu
- Estrada, Adrián (2005); Protocolos TCP/IP, CISCO. *Tecnología y diseño*. Recuperado en: https://goo.gl/c6GJPt
- EU2017.EE, Speech by Estonian Prime Minister Jüri Ratas: a review of the Estonian Presidency. *EU2017*. Recuperado en: https://goo.gl/YTgDCi
- European Comission. Infraestructure-TEN-T-Connecting Europe. *Mobility and Transport*. Recuperado en: https://goo.gl/GEChZL
- Kaspersky Lab. Cyberthreats Map. *Kapersky.* Recuperado en: https://goo.gl/kNvWNh
- Malknecht, Greg (2010), Mapa de cables submarinos. *Cablemap.* Recuperado en: https://goo.gl/ZshhWz
- Mapa Carreteras (2016). Guía de caminos y carreteras en Alemania. Recuperado en: https://goo.gl/Zay2kH
- Naciones Unidas. Capítulo VII: Acción en caso de amenazas a la paz, quebrantamientos de paz o actos de agresión. *Carta de Naciones Unidas.* Recuperado en: https://goo.gl/c4ufSj
- Victoria, Luis (2012). La historia del comercio electrónico. *Lynkoo*. Recuperado de: https://goo.gl/jcH5Nq

Videos

- Duke University School of Law [LENS] (2013), Conference 2013 Michael N. Schmitt, The Law of Cyberwar: The Tallinn Manual [Archivo de video], Recuperado de: https://goo.gl/DHdmBZ
- NATO [USNAVALWARCOLLAGE] (2012), CyCon 2012, Michael Schmitt: Tallin Manual Part I [Archivo de video], Recuperado de: https://goo.gl/UC1qt9
- NATO [USNAVALWARCOLLAGE] (2012), CyCon 2012, Michael Schmitt: Tallin Manual Part II [Archivo de video], Recuperado de: https://goo.gl/U9zU5P
- NATO [USNAVALWARCOLLAGE] (2012), CyCon 2012, Michael Schmitt: Tallin Manual Part III [Archivo de video], Recuperado de: https://goo.gl/idsyD9
- NATO [USNAVALWARCOLLAGE] (2012), Wolff Heintschel von Heinegg: Sovereignty in Cybersace [Archivo de video], Recuperado de: https://bit.ly/2EXyEmG
- NATOCCDCOE [NATOCCDCOE] (2016), Tallin Manua 2.0 Approach to State Responsibility [Archivo de video], Recuperado de: https://goo.gl/eZK5qU
- NATOCCDCOE [NATOCCDCOE] (2015), Tallin Manual Experts Meet for Intense Drafting Session [Archivo de video], Recuperado de: https://goo.gl/muHz54
- NTN24 [NTN24] (2013), Manual de Tallin explica cómo los Estados podrían defenderse de los ciberataques [Archivo de video], Recuperado de: https://goo.gl/1rCk93
- Palo Alto Networks [Palo Alto Networks] (2016), 2016 Cyber Canon Inductee-Tallin Manual [Archivo de video], Recuperado de: https://goo.gl/wNVcE4
- The University of Adelaide [Army Cyber Institute] (2016), Tallin Manual 2.0 Panel [Archivo de video]. Recuperado de: https://goo.gl/JYUpJJ

- The University of Adelaide [Cyber101x Cyberwar] (2015), Surveillance and Security, Tallin Manual on cyberoperations [Archivo de video], Recuperado de: https://goo.gl/7QF6pL