LA CIBERSEGURIDAD COMO FACTOR CRÍTICO EN LA SEGURIDAD DE LA UNIÓN EUROPEA

Nieva Machín[1] y Manuel Gazapo[2]
UNISCI

Resumen:

El ciberespacio es un escenario de conflicto altamente complejo al estar en constante evolución. Ni la Unión Europea ni ningún otro actor del sistema internacional se encuentra a salvo de las amenazas procedentes del ciberespacio. Pero los pasos dados desde la UE en el mundo de la ciberseguridad no son en absoluto suficientes. Europa necesita que su Estrategia de ciberseguridad sea realmente capaz de integrar a las diferentes Estrategias nacionales. Es urgente una mayor determinación, unos mayores recursos y unos mejores instrumentos que permitan a la Unión implementar una gestión de crisis y una prevención de ciberconflictos verdaderamente eficaz.

Palabras clave: Ciberespacio, ciberseguridad, Estrategia Europea de Ciberseguridad, Estrategia Global de Seguridad de la Unión Europea

Title in English: *Cybersecurity as a critical factor for the Security of the European Union*

Abstract:

Cyberspace is a very complex conflict scenario in constant evolution. Neither the European Union nor any other actor of the international system is safe from cyberspace threats. But the steps taken in the EU on cyber-security are clearly insufficient. Europe needs a cyber-security Strategy really able of integrating the different national Strategies. It is urgent to have a stronger determination, more resources and better tools, allowing the Union to implement efficient crisis management and cyber-conflict prevention.

Keywords: *Cyberspace, cybersecurity, European Cyber-security Strategy, Global Security Strategy of the European Union.*

[1] La Dra. Nieva Machín Osés es investigadora senior de UNISCI, profesora universitaria en el grado oficial de criminología. Actualmente desempeña su labor como docente universitaria en diversos centros universitarios así como la dirección y coordinación de los programas máster del área de Internacional en IMF.
E-mail: nieva@hotmail.es

[2] Manuel Gazapo Lapayese es Director del International Security Observatory y miembro del Grupo de Investigación de Paisaje Cultural de la Universidad Politécnica de Madrid.
E-mail: m.gazapo.lapayese@hotmail.com
DOI: http://dx.doi.org/10.5209/RUNI.53786

1.Introducción.

Desde finales del siglo XX la sociedad ha sufrido una transformación sin parangón en la historia de la humanidad debido a la irrupción de internet; esta ha supuesto toda una revolución que ha transformado las relaciones entre los individuos, las relaciones entre actores estatales y comerciales, e incluso los dispositivos que utilizamos para realizar dichas interacciones. Esta revolución está vinculada al surgimiento de una nueva dimensión, el denominado ciberespacio, donde todo este tipo de interacciones afectan tanto a los derechos fundamentales como a la economía. Por lo tanto debe entenderse el ciberespacio no tanto como un escenario o una dimensión aséptica, abstracta y distanciada de los seres humanos, sino todo lo contrario, el ciberespacio se caracteriza por ser un mundo vaporoso, rizomático, abierto y múltiple, donde nos interrelacionamos.

El ciberespacio ha trascendido las limitaciones propias de las fronteras entre los países; los ciudadanos interaccionan e intercambian información e ideas con una libertad e inmediatez como jamás había sido posible; se ha proporcionado un foro para la libertad de expresión y el ejercicio de los derechos fundamentales. Según se afirma desde la Unión Europea[3] "el ciberespacio, tiene una naturaleza inherentemente transnacional; consta de una serie de redes e infraestructuras interdependiente. Por ejemplo, entre otras, internet y las redes de telecomunicación, constituyen uno de los canales presentes y futuros más importantes para satisfacer las necesidades, intereses y derechos de los ciudadanos de la UE y de sus Estados miembros constituyéndose en un activo indispensable del crecimiento económico de la UE."

Internet se ha convertido, sin duda alguna, en un elemento clave para el crecimiento económico, además de en un recurso crítico del cual otros sectores económicos y productivos dependen tales como las operaciones bancarias/financieras tanto nacionales como internacionales, infraestructuras y medios de transporte, el sector energético y el sanitario. Debido al alto grado de dependencia que estos sectores presentan de internet y de las tecnologías de la información y de la comunicación (TIC), un fallo en la red o una incidencia sobre la misma podría suponer una vulnerabilidad y/o amenaza en materia de seguridad, bien de índole energética, sanitaria, económica….etc. Todo ello destaca la necesidad de realizar acciones que doten a esta nueva realidad de una estrategia de ciberseguridad. A nivel internacional, la ciberdefensa y la ciberseguridad están declaradas como unas de las mayores prioridades en términos de seguridad, ya que uno de los retos a nivel global en la actualidad es la necesidad de poder tratar adecuadamente la información. Se trata de un tema de incuestionable relevancia ya que cada vez aumenta en mayor medida la dependencia en torno a los medios cibernéticos. Como se podrá observar a lo largo del análisis, el desarrollo de la actividad cibernética ha proporcionado innumerables beneficios a la sociedad. Sin embargo, no podemos obviar que la rapidez con la que evolucionan las tecnologías, sumado al ritmo con el que se expande el ciberespacio, no permite desarrollar los mecanismos adecuados para prevenir de forma eficaz y eficiente las ciberamenazas: los ataques cibernéticos vulneran las políticas establecidas en Europa, por lo que se puede afirmar sin lugar a dudas que es el actual talón de Aquiles de nuestra sociedad.

[3]Unión Europea (2013): *"Conclusiones del Consejo sobre la comunicación conjunta de la Comisión y de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, titulada "Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro"*. nº 12109/13, en http://register.consilium.europa.eu/doc/srv?f=ST+12109+2013+INIT&l=es

2. Traslación del conflicto a la dimensión virtual.

Ha de entenderse el ciberespacio como un conjunto de dispositivos conectados por redes en las que se almacena y se utiliza la información electrónica así como el espacio donde diversos actos comunicativos tienen lugar. Otro enfoque que debemos dar a la definición del ciberespacio es la comprensión de la naturaleza del mismo y el propósito de este, siendo este último el procesamiento, manipulación y la explotación de la información, la facilitación y el aumento de la comunicación entre los individuos y la interacción entre personas y la información. De ahí se desprende la idea de que tanto la información como las personas son elementos fundamentales en la composición del ciberespacio, por tanto, individuos e información son susceptibles de sufrir amenazas o presentar vulnerabilidades.

El ciberespacio es un dominio caracterizado por el uso de los datos y la electrónica para poder almacenar, enviar o modificar información, gracias a los sistemas en red e infraestructuras físicas asociadas. Estando este compuesto por los cuatro elementos principales que podemos ver en la siguiente figura.

Figura 1 Elementos del ciberespacio

Fuente: Elaboración propia basada en la información expuesta en el artículo de Styktz y Banks: "Cyber Warfare Simulation to Prepare to Control Cyber Space"

De hecho, el ciberespacio puede ser pensado como la interconexión de los seres humanos a través de las telecomunicaciones, sin tener en cuenta la geografía física. La complejidad de la naturaleza del ciberespacio junto con que este es cada vez más dinámico, incierto y complejo nos lleva a tratar de delimitar que es a lo que debe considerarse un ataque cibernético. De acuerdo con la figura anterior, un ciberataque es aquel que se realiza contra uno o más de los cuatro elementos que conforman el ciberespacio y que se perpetre con el fin de tener acceso o manipular la información de un adversario. Siendo el objetivo de este ciberataque incidir en la percepción y conciencia que el adversario tiene de la situación y en su proceso de toma de decisiones, así como conducir al adversario a tomar decisiones deseadas. Un ataque cibernético supone una incidencia en el nivel del conocimiento de la situación, tanto a nivel individual como grupal, así como de mando y control, al socavar uno o más elementos del

ciberespacio.[4] Teniendo en cuenta la premisa de que un ciberataque supondría una ofensiva a uno a más de los elementos mencionados anteriormente, cabe pensar que los ataques cibernéticos serán coordinados y podrán ser elaborados con el fin de maximizar la confusión[5].

El ciberespacio, por tanto, debe ser protegido de incidentes, actividades maliciosas y un mal uso. Los gobiernos tienen un papel importante para garantizar un ciberespacio libre y seguro; estos han de realizar diversas tareas para conseguirlo, siempre respetando y protegiendo los derechos fundamentales de los ciudadanos en internet y mantener la fiabilidad y la interoperabilidad en el ciberespacio. En aras de proporcionar a la ciudanía un ciberespacio abierto y libre, deben estar vigentes en él la misma normativa, principios y valores que defiende la Unión Europea fuera del ciberespacio. Los derechos fundamentales, la democracia y el Estado de derecho necesitan ser protegidos en el ciberespacio. Nuestra libertad y la prosperidad dependen cada vez más de un robusto e innovador ciberespacio así como de todos los avances vinculados a internet que continuaran apareciendo, si los procesos de investigación e innovación del sector privado y la sociedad civil impulsan su crecimiento. Pero la libertad en el ciberespacio requiere de protección y seguridad.

El sector privado posee y opera una parte significativa del ciberespacio gracias a la revolución digital, favoreciendo esta revolución la innovación empresarial, el crecimiento económico y comercial en Europa. Esta situación también lleva consigo exponer a las organizaciones a nuevas amenazas y riesgos informáticos. A medida que las organizaciones adoptan dinámicas vinculadas a entornos digitales las organizaciones son cada vez más difíciles de defender. Esto se debe al efecto de los siguientes factores[6]:

a) La consumerización[7], entendida esta como la tendencia en la cual los entornos digitales y las tecnologías de la información y la comunicación tienen una mayor difusión e índice de penetración entre la población, los individuos, los consumidores y ciudadanos para posteriormente propagarse hacia las organizaciones comerciales y gubernamentales. El impacto más relevante de la consumerización en ciberseguirdad es que está incidiendo en que las empresas se planteen el modo en que adquieren y administran sus servicios así como sus equipos tecnológicos. Las empresas cada vez más adquieren plantillas para la realización de sus websites y tiendas online así como software de gestión que requieren una mínima adaptación o bien permiten actualizaciones en la nube incluyendo tanto la compraventa online como la actualización de software y apps. La consumerización permite enfoques alternativos y una simplificación de la operativa o gestión de las empresas, pero también está suponiendo una vulnerabilidad en materia de ciberseguridad.

b) El incremento de la colaboración y el intercambio multiplataforma de grandes volúmenes de datos sensibles.

[4] Martin R, Stytz.; Sheila B. Bank (2014): "Cyber Warfare Simulation to Prepare to Control Cyber Space". *National Cybersecurity Institute Journal*, vol 1, nº2. p. 9.
[5] Lynn, William J.: "Defending a new domain: The Pentagon's cyberstrategy" *Foreign Affairs* , vol.89, nº.5, (September-October 2010).
[6] Hurtaud, S (2014):"Cyber security Time for a new paradigm". *Information & Technology Risk*. Ed. Deloitte, pp. 90-95
[7] Término creado por Douglas Neal y John Taylor. La primera publicación sobre este tema fue "La consumerización de la tecnología de la información", publicado por el "LEF" en junio de 2004. Special Report: Personal Technology, "Consumerisation: The Power of Many", *Economist*, 8 October 2011, en http://www.economist.com/node/21530921

c) La innovación tecnológica y su rápida difusión está suponiendo una falta de comprensión por todos los actores, tanto gubernamentales como comerciales así como ciudadanos.

d) La trivialización de los efectos en materia de seguridad de la actividad de las organizaciones en el ciberespacio como, por ejemplo, la computación en la nube.

e) Incidencias en la reputación e imagen de la organización. Un ataque cibernético puede suponer un perjuicio a la reputación ya que, dependiendo de la naturaleza del ataque, éste destruye la confianza de los consumidores e incluso de los ciudadanos si la entidad que ha sufrido el ciberataque es un organismo público.

f) El fenómeno de la globalización y la supresión de las fronteras en internet ha supuesto el surgimiento de nuevas amenazas que surgen gracias a la presencia global online, la expansión en nuevos mercados de las organizaciones.

Tras haber visto los factores que inciden en que las organizaciones adopten dinámicas vinculadas a entornos digitales se estén volviendo más difíciles de defender, resulta oportuno destacar que el ciberespacio actualmente es un entorno virtual habilitado por una infraestructura digital mundial generalizada. Esta ofrece un escenario ideal para la realización de actividades comerciales, habiendo facilitado e impulsado el comercio internacional y habiendo transformado el comercio de productos culturales, así como la actividad científica y sobre todo su divulgación; sin olvidar el impulso que ha supuesto a la educación, la comunicación y las actividades de origen político, desde la difusión propagandística de diversos idearios hasta la agilización de gestión de tramites entre gobierno y ciudadanos. El ciberespacio a nivel económico y social supone un lugar de oportunidades de negocio y la plataforma de difusión cultural por excelencia pero también una amenaza a la seguridad individual, colectiva, nacional e internacional. A medida que las organizaciones del sector público y privado siguen derivando sus actividades al entorno digital, es decir, al ciberespacio, también lo hacen las organizaciones criminales. Cabe entonces plantearse la definición de delito cibernético, siendo este el término destinado a aquellas actividades delictivas llevadas a cabo mediante el empleo de un ordenador o de internet. La actividad delictiva se ha tornado más sofisticada, por lo que cada vez resulta más difícil detectarla y combatirla. Siendo la cuestión de la ciberseguridad una cuestión inquietante tanto para las organizaciones comerciales, como para los Estados y los ciudadanos.

A nivel internacional, la ciberseguridad está cobrando unos marcados matices de relevancia y de urgencia, a medida que la economía digital se ha ido desarrollando en los últimos 15 años, las empresas así como los consumidores son más dependientes que nunca de los sistemas de información. La relevancia de la ciberseguridad sigue viéndose incrementada debido a la aparición de una nueva ola de sistemas ciber-físicos como son los dispositivos "inteligentes" para el hogar, vehículos autónomos y sistemas aéreos no tripulados. Sin embargo, en este contexto de transformación digital, es cada vez más claro que tanto el público como el sector privado no pueden seguir el ritmo de las amenazas de ciberseguridad. Para abordar este problema generalizado, desde la Unión Europea y desde los gobiernos de todos los países que la conforman precisan alinear sus esfuerzos en materia de ciberseguridad para hacer frente a esta nueva realidad.

2.1 Razones que justifican la traslación de los conflictos al ciberespacio.

La principal razón por la que los conflictos se están trasladando al ciberespacio es la rentabilidad económica**.** Un equipo informático bien sea un ordenador o un smartphone puede ser utilizados como un arma de bajo coste frente a las convencionales, siendo estos

dispositivos muy efectivos, teniendo en cuenta el alcance que se puede conseguir con su uso. Los avances informáticos han posibilitado que un individuo que use un ordenador como arma pueda realizar acciones con la posibilidad de interferir en las dinámicas comerciales, financieras, de infraestructuras e incluso en los equipos médicos, teniendo la potencialidad de causar graves daños a un individuo, una organización comercial o gubernamental. Asociado al bajo coste de los dispositivos como arma, es importante destacar los mínimos costes que suponen el mantenimiento y reposición de los mismos.

Otra de las razones es la gran capacidad operacional y flexibilidad operativa con las que se cuenta operando en el ciberespacio, debido a que se pueden perpetrar más ataques en menos tiempo que en el espacio convencional, teniendo como efecto una merma en los tiempos de reacción.

En cuanto al alcance, este es ilimitado debido a la cobertura global de los satélites. Siendo un elemento más que está favoreciendo que los conflictos se estén trasladando de escenario es que en el ciberespacio la coordinación de un ataque es más fácil así como que en el ciberespacio el anonimato e ineficacia de los procesos de atribución son posibles ya que internet posibilita que cualquier individuo desde cualquier ubicación geográfica pueda perpetrar un ciberataque de un modo anónimo y de difícil rastreo, complicando las actividades forenses cibernéticas. Siendo por tanto muy difícil la identificación del delincuente. Esto supone una ventaja clara respecto a la actividad delictiva convencional, en la cual la imputación de una actividad delictiva a un individuo, grupo o actor estatal es más accesible. Esto tiene como consecuencia que se verá dificultada la capacidad de realizar contraofensivas de la víctima que haya sufrido el ciberataque.

Ante todo este panorama esbozado sobre el porqué los conflictos están trasladándose al ciberespacio, cabe señalar como una de las más importantes la insuficiencia del derecho internacional**.** Nos enfrentamos actualmente a una gran laguna normativa internacional en el ámbito de la jurisdicción competente en materia de delitos informáticos, lo cual está siendo origen en sí mismo de conflictos y de inseguridad. En el panorama actual el sujeto activo puede cometer un delito desde un Estado diferente al que se encuentra el sujeto pasivo. Frecuentemente resulta difícil determinar cuál es la legislación nacional que está siendo violada debido a que la ubicación del contenido difundido a través de la red es simultánea y de acceso global. Por esta razón, las actividades desarrolladas y difundidas por internet cobran un carácter internacional que pudieran involucrar a múltiples jurisdicciones[8].

Esto suscita problemas como, por ejemplo, la diferente regulación del Derecho sustantivo[9] en los distintos Estados. Esto ha generado una situación muy complicada ya que determinados actos son punibles según la legislación de un Estado, pero no de otro, dando lugar a obvias desigualdades y zonas de impunidad. [10]

[8] Kurbalija, J; Gelbstein, E.(2005):"Gobernanza de Internet: Asuntos, Actores y Brechas", Ed. DiploFoundation, pág 82 en http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1090

[9] El derecho sustantivo hace referencia a una serie de normas, preceptos o pautas que demandan los derechos y obligaciones de los individuos que contienen nexos con el orden jurídico propuesto por el Estado. El derecho sustantivo se encuentra anexado en normas de contenido sustantivo, tales como el Código Penal o el Código Civil, entre otros.

[10] Diaz Gómez, A.(2010):"El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest", *REDUR 8*, Diciembre 2010, pp. 169-203.

3. Riesgos y amenazas de la ciberseguridad.

En el contexto internacional actual, podemos observar que los ataques cibernéticos pueden afectar tanto a ordenadores, teléfonos móviles como a redes informáticas inalámbricas. No existe límite ni barrera que impida a los ciberatacantes introducirse en todos aquellos entes que tengan una conexión con el ciberespacio.

Los ciberataques utilizan las brechas de seguridad presentes en las tecnologías de información para pasar a copiar, borrar o reescribir la información de la víctima y se aprovechan de las vulnerabilidades que presentan la mayor parte de las estructuras cibernéticas como, por ejemplo, las redes sociales. En el siglo XXI los bits y los bytes pueden ser tan amenazantes como las balas y las bombas[11]. El número y variedad de los ciberataques puede llegar a ser extremadamente alto, debido a la continua evolución y metamorfosis de los instrumentos informáticos cuya complejidad es cada vez más elevada. En consecuencia, hemos elaborado una lista en la que se van a describir las amenazas o ciberataques más extendidos hasta la fecha:

- Código dañino: se trata de la amenaza más común dentro del ciberespacio. Conocido también como código malicioso o malware, tiene su fin principal en dañar el funcionamiento correcto de cualquier equipo informático, ya sea inutilizando el sistema operativo o haciéndose con el control de la memoria.

- Gusano: se trata de códigos dañinos calificados como independientes, al estar diseñados para reproducirse a sí mismos, es decir, realizar copias de sí mismo y enviarlas a todos aquellos ordenadores que estén conectados a través de la red.

- Virus: consiste en un programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.

- Troyano: es un software que suele aparentar ser inofensivo o incluso realizar tareas necesarias para el usuario, pero que en realidad su objetivo es el robo o destrucción de la información acumulada en el dispositivo.

- Botnet: es un conjunto de software que permite llevar a cabo ataques de denegación de servicio, fraudes, robos de información, la inutilización de los sistemas de antivirus o detección de intrusos o la perturbación del comercio electrónico.

- Bomba lógica: son ciberataques cuya finalidad no es extenderse ni actuar continuamente, sino pasar a la acción en un momento determinado preestablecido por el atacante. En consecuencia, su duración es limitada en el tiempo al realizar sus funciones dañinas únicamente cuando se ha llegado al momento o cantidad de visitas preestablecidas.

Los atacantes pueden clasificarse atendiendo a diversas categorías como la autoría o la motivación. Pero es desde la autoría desde donde podemos, de forma más contundente y operativa, trazar una posible clasificación de los atacantes que nos permita una lectura de este nuevo escenario de conflicto:

- Estados: Aunque pueda parecer llamativo, el hecho de que los Estados pueden ser el origen de numerosas amenazas cibernéticas ha provocado que la complejidad de la situación en la que se encuentra el ciberespacio aumente considerablemente. Esta situación muestra que muchos Estados como China, Rusia, Estados Unidos o Israel,

[11] Gómez, Ángel (2012): "El ciberespacio como escenario de conflicto. Identificación de las amenazas", en *El ciberespacio. Nuevo escenario de confrontación*, Madrid, Ed. Ministerio de Defensa, pp. 167-204.

han tomado conciencia de la ventaja comparativa que les puede brindar el desarrollo de armas cibernéticas, por lo que podemos predecir que el aumento exponencial de la complejidad de los ciberataques se va a ver aún más potenciado a consecuencia de la inversión procedente de los Estados.

- Empresas: no se debe olvidar a estos agentes económicos como una de las principales fuentes de ciberataques: El espionaje industrial y el espionaje comercial.

- Terrorismo: los conflictos tradicionales y sus actores se han desplazado al ciberespacio como nuevo escenario de enfrentamiento[12]. Esto ha provocado que los grupos terroristas y los grupos extremistas religiosos, encuentren en el ciberespacio un escenario donde llevar a cabo sus ataques y sus tareas de propaganda, captación o adoctrinamiento de potenciales terroristas.

- Delincuencia organizada: la desmaterialización de las transacciones en el ciberespacio, la gran cantidad de recursos presentes en la nube, la existencia de fallos en los sistemas de comercio electrónico y los mercados financieros, y la inexistencia de un marco jurídico armónico entre los Estados que haga frente a las amenazas procedentes del ciberespacio, ha invitado a la redes del crimen organizado a identificar al ciberespacio como un escenario propicio en el que llevar a cabo sus operaciones. Ejemplo de ello es la banda Carbanak, la cual consiguió robar 876 millones de euros de un centenar de bancos e instituciones financieras en 30 países[13].

- Hacktivismo: este fenómeno también conocido como piratería informática podríamos interpretarlo como la utilización de las herramientas informáticas para la acción política no violenta, es decir, la utilización de los recursos y medios que ofrece el ciberespacio para llevar a cabo protestas notorias tanto de carácter político, económico o social. Sus herramientas incluyen desde desfiguraciones hasta el robo de información y sabotajes virtuales.

Se trata de un fenómeno que ha sufrido un enorme crecimiento en los años posteriores al surgimiento de actual la crisis económica: ejemplo de ello son los grupos o actores como WikiLeaks o Anonymous, quienes han llevado a cabo ciberataques dirigidos a la consecución de una denegación de servicio, la destrucción de datos o la publicación de información confidencial a modo de protesta en contra de determinados gobiernos. Ahora bien, cabe destacar que hay otra corriente dentro de este movimiento que lo que pretende es la búsqueda y evidencia pública de fallos en la ciberseguridad con la finalidad de que estos sean solventados. Ejemplo de ello es el caso del Chaos Computer Club, un grupo de hacktivistas alemanes especialistas en hacer demostraciones públicas de seguridad sin intenciones maliciosas. Este grupo consiguió que un banco les hiciera una transferencia por valor de 67.000 euros a sus cuentas, haciendo la devolución de la suma delante de la prensa[14].

3.1 Infraestructuras críticas

Recientes ciberataques han demostrado que los ataques virtuales tienen un impacto muy significativo en las infraestructuras y servicios críticos, pudiendo causar consecuencias

[12] Torrecuadrada, Soledad (2013): "Internet y el uso de la fuerza", en *Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio,* Granada, Ed. Universidad de Granada, pp. 91-118.
[13] Sanger, David and Perloroth, Nicole: "Bank Hackers Steal Millions via Malware", *New York Times*, 14 February 2015, en http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=1
[14] Bulnes, Ana: "Más allá de Anonymous: censo de grupos hacktivistas" *Silicon*, 28 de junio de 2011, en http://www.silicon.es/mas-alla-de-anonymous-censo-de-grupos-hacktivistas-2196485#4ivLHhMoWFCZz82b.99

desastrosas para los Estados miembros de la Unión Europea y el bienestar social. En concordancia con la hipótesis planteada, en los siguientes epígrafes vamos a tratar de concretar esa dimensión tangible del ciberespacio en materia de seguridad en las áreas de las infraestructuras críticas, la identificación de individuos gracias a la implementación del control biométrico y su aplicación en materia de terrorismo, el sector financiero y el sanitario.

En cuanto a la defensa de las infraestructuras criticas, 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 protección adecuada de las mismas así como el empleo efectivo en materia de comunicaciones durante las operaciones desplegadas en entornos hostiles. Frecuentemente 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. Respecto a la cuestión de la ciberseguridad, esta situación manifiesta una serie de retos en materia de gestión de riesgos, la aplicación de las normas de seguridad y la garantía de servicio a las aplicaciones críticas[15].

Las infraestructuras críticas, así como las plantas de generación de electricidad, los sistemas de transporte y las instalaciones de fabricación son controlados y supervisados por sistemas industriales de control (ICS), incluyendo el SCADA (Supervisión, Control y Adquisición de Datos) un software que permite el control y supervisión de los procesos industriales de manera remota. Este ofrece una retroalimentación a tiempo real con los dispositivos de campo, controlando el proceso de manera automática. La implementación de estos sistemas incrementa tanto la operatividad y eficiencia ya que permite una optimización de los recursos. Aunque también suponen una mayor exposición a los ciberataques ya que estos sistemas podrían ser intervenidos maliciosamente.

Esta mejora en las operaciones y servicios está suponiendo la exposición de toda la red de energía eléctrica a los nuevos desafíos en el campo de la seguridad de las redes de comunicación y sistemas de información. La vulnerabilidad de estas redes puede suponer el sabotaje de las mismas causada por motivos financieros o políticos. Pueden ser acciones que causen cortes de energía a grandes áreas o bien perpetrar ataques cibernéticos contra las plantas de generación de energía.

En cuanto a las infraestructuras y el transporte cabe destacar el sector marítimo, ya que es clave para la sociedad europea. El transporte internacional naval aporta el 74% de las mercancías de fuera de la Unión Europea. Europa cuenta con más de mil doscientos puertos comerciales en sus costas. Los puertos son esenciales para la actividad de transporte así como para la competitividad de Europa, teniendo un enorme potencial en la creación de puestos de trabajo y de inversión. Europa es una de las regiones con mayor densidad portuaria del mundo, cada año por los puertos europeos transitan el 37% del tráfico intracomunitario de mercancías y unos 385 millones de pasajeros[16].

Las tecnologías de la información y la comunicación (TIC) se utilizan cada vez más para permitir las operaciones marítimas esenciales, desde la navegación a la propulsión, desde la gestión de la carga de comunicaciones de control de tráfico, etc.

[15] Robinson, N.(2014): "EU cyber-defence: a work in progress". *EU Institute for Security Studies*, vol.10, marzo 2014, pp 1-10, en http://www.iss.europa.eu/uploads/media/Brief_10_Cyber_defence.pdf

[16] Comisión Europea (2013): "Los puertos marítimos de Europa en el horizonte de 2030: retos futuros". Bruselas, 23 de mayo de 2013, en http://europa.eu/rapid/press-release_MEMO-13-448_es.htm

La conciencia de ciberseguridad marítima es muy poca. Los Estados miembros de la Unión Europea deberían llevar a cabo la sensibilización del sector marítimo realizando actividades de concienciación y formación en seguridad cibernética de las compañías navieras, autoridades portuarias, etc. Debido a la alta complejidad de las TIC que intervienen el todo el proceso, esto tiene como consecuencia que asegurar los niveles adecuados de ciberseguridad marítima resulte muy importante. Los reglamentos y las políticas marítimas actuales consideran sólo los aspectos físicos de la seguridad, por lo que los legisladores deberían añadir los aspectos de seguridad cibernética. Se ha de realizar una evaluación de los riesgos cibernéticos y la identificación de los activos críticos dentro de este sector. La Organización Marítima Internacional, junto con la Comisión Europea y los Estados miembros deben alinear las políticas internacionales y de la UE en este sector.[17]

3.2 Los controles biométricos.

El atentado de Paris del 7 de enero del 2015 suscitó la necesidad de analizar las iniciativas de introducir controles más estrictos en los pasos de acceso para ciudadanos Schengen en los aeropuertos europeos, sobre todo pensando en el regreso de los individuos con ciudadanía europea que regresan a Europa tras combatir en el Daesh. Debido a que en la actualidad los controles más exhaustivos se realizan a los extranjeros y eso puede suponer una vulnerabilidad para la seguridad europea. Para ello podría resultar muy útil la incorporación de las nuevas tecnologías a los procesos de identificación y autentificación de las personas gracias a las técnicas biométricas, ya que la biometría garantiza uno de los niveles de autenticación menos vulnerables. Los controles biométricos pueden utilizarse no únicamente para el proceso de autentificación de la identidad sino para identificar posibles ejecutores de ataques terroristas.

Figura 2. Controles Biométricos

TECNOLOGÍA	APLICACIONES EN SEGURIDAD
AFIS/Lifescan	Controles de Vigilancia, Servicios policiales y militares
Reconocimiento de cara	Identificación sin contacto
Geometría de Mano	Identificación Criminal, Sanidad.
Reconocimiento de iris	Acceso a sistemas
Reconocimiento de Voz	Acceso a instalaciones
Escritura y Firma	Vigilancia

Fuente: Elaboración propia.

La aplicación de la biométrica a las TIC y la ciberseguridad está siendo una tendencia que está creciendo exponencialmente en los últimos meses ya que la combinación del empleo de estas técnicas incrementa el nivel de seguridad. A continuación se presenta una tabla comparativa de los sistemas biométricos[18]:

[17] ENISA (2011):"Cyber Security Aspects in the Maritime Sector" en https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

[18] Tapiador.Marino, Sigüenza.Juan Alberto (2005):" Tecnologías biométricas aplicadas a la seguridad", Madrid, ed. RA-MA.

Tabla 1 Sistemas biométricos

	Ojo (Iris)	Retina	Huellas dactilares	Vascular dedo	Vascular mano	Geometría de la mano	Escritura y firma	Voz	Cara 2D	Cara 3D
Fiabilidad	Muy alta	Muy Alta	Muy Alta	Muy Alta	Muy Alta	Alta	Media	Alta	Media	Alta
Facilidad de uso	Media	Baja	Alta	Muy Alta	Muy Alta	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy Alta	Alta	Muy Alta	Muy Alta	Alta	Media	Media	Media	Alta
Aceptación	Media	Baja	Alta	Alta	Alta	Alta	Muy Alta	Alta	Muy alta	Muy alta
Estabilidad	Alta	Alta	Alta	Alta	Alta	Media	Baja	Media	Media	Alta

Fuente: Tapiador.M; Sigüenza.J. (2005). Tecnologías biométricas aplicadas a la seguridad.

Tras los atentados del 7 de Julio del 2005 en Londres, el gobierno británico reconsideró las medidas de seguridad y revisó el sistema estatal de prevención de actos de terrorismo en el transporte incorporando exitosamente cámaras de vigilancia "inteligentes". En España ya está implantada la biometría facial en el aeropuerto de Barajas, usando las cámaras de seguridad del aeropuerto para el reconocimiento de personas, cuya identidad era contrastada con una base de datos facial[19].

En Noruega, la policía ha estado utilizando la tecnología de control biométrico (el sistema EasyPass) en el aeropuerto de Gardermoen asegurándose de que los rasgos faciales de los pasajeros se ajustan a la fotografía en el pasaporte.

Las fuerzas y cuerpos de seguridad de diversos países han mostrado interés en la tecnología biométrica desarrollado en el año 2012 por la japonesa Hitachi Kokusai Electric. Esta tecnología consiste en un sistema de cámaras biométricas que es capaz de escanear 36 millones de rostros por segundo. El sistema que han elaborado permite que las cámaras recopilen imágenes de cientos de miles de personas presentes en determinadas ubicaciones de acumulación masiva generando una base de datos con las imágenes de todas las caras escaneadas. A continuación, los datos se clasifican en base a los criterios biométricos para facilitar la búsqueda de una cara específica.[20]

Muchos son los países que han optado por la introducción del control biométrico para mejorar las medidas de lucha contra el terrorismo, entre ellos destaca Estados Unidos ya que recopila datos biométricos en Irak, Afganistán y otros lugares. Estos datos incluyen huellas digitales, exploraciones de retina y otros indicadores biométricos como por ejemplo muestras de ADN. Unas veces estos datos biométricos se asocian con una identidad concreta y otras, cuando los datos forenses son recogidos en el lugar donde ha estallado la bomba la relación entre los datos y la identidad biométrica es desconocida, siendo este último supuesto bastante frecuente.[21]

[19] Conde Vilda, C et al (2007); "Biometría facial en el aeropuerto de Barajas". *Perspectiva Empresarial.* ed. Universidad Rey Juan Carlos, nº9, abril 2007; pp. 94 y 96-97.
[20] " Una cámara de vídeo que reconoce una cara entre 36 millones... en un segundo". *El Mundo*, 26 de marzo 2012 en http://www.elmundo.es/elmundo/2012/03/26/navegante/1332752448.html
[21] Center for Strategic and International Studies (CSIS).(n.d) :"Biometrics and Security" en https://www.csis.org/programs/strategic-technologies-program/cybersecurity/other-projects-cybersecurity/biometrics-and

En el escenario internacional donde los conflictos actuales, las distinciones entre las fuerzas extranjeras y nacionales así como las delimitaciones entre la ley, la defensa y la inteligencia se han desdibujado, se requiere la articulación de reglas que permitan la recopilación y gestión de los datos biométricos registrados así como mecanismos de cooperación que posibiliten el compartir esta información entre los diferentes organismos e incluso diferentes gobiernos.

3.3 Sector financiero.

El sector financiero constituye un pilar fundamental de la economía europea y su dependencia es cada vez mayor en las infraestructuras TIC hace que este sector presente un elevado grado de vulnerabilidad. La protección de las transacciones interbancarias automatizadas así como el resto de operaciones financieras realizadas en base a las TIC ha convertido a la ciberseguridad en un elemento crítico de este sector.

Un sistema financiero estable en Europa es la base fundamental para la estabilidad económica. La cooperación entre los actores clave del sector financiero a nivel paneuropeo se convierte en una necesidad urgente ya que el sector se enfrenta a retos cada vez mayores y de mayor escala.

La protección de bancos e instituciones financieras presenta diversos inconvenientes: la aplicación de una multitud de normas técnicas y de seguridad difíciles de mantener; la pérdida de interoperabilidad; la imposibilidad de implementar un "Safe Habouring"[22] así como la asistencia y ayuda mutua; el hosting o más tipos de sistemas, menos seguros; así como la vulnerabilidad general a los ataques cibernéticos.[23]

Completando lo anteriormente señalado el sector de los servicios financieros y al por menor debería dar prioridad a los ataques procedentes de las siguientes fuentes, destacando por su alto porcentaje los archivos adjuntos en los emails recibidos así como los link recibidos mediante email.[24]

Respecto a tipología de datos comprometidos en las actividades de ciberespionaje destacando entre ellos la información confidencial con un 85.5%.[25]

3.4 Sector sanitario.

Otro elemento de las infraestructuras críticas susceptibles de sufrir ciberataques es el sector sanitario y más concretamente lo que actualmente se denomina e-salud, el cual afecta tanto en el sector privado y público. Debido a que los servicios de salud han sido reconocidos como una función social fundamental, es importante analizar el grado en que los distintos sistemas de salud electrónica y las infraestructuras son cruciales para la prestación segura de estos servicios.

La complejidad de los sistemas de salud "on line" es muy elevada lo que hace que la calidad de la información, la accesibilidad y la disponibilidad sea una tarea muy difícil. Los EHR (registros electrónicos de salud) o PHR (registros de salud del paciente) que son

[22] Un *safe harbor* es una disposición de una ley o reglamento que especifica que cierta conducta no viola una norma

[23] ENISA (2015): "Secure Use of Cloud Computing in the Finance Sector" en https://www.enisa.europa.eu/publications/cloud-in-finance.

[24] *Ibid.*

[25] *Ibid.*

esquemas de intercambio de datos de salud, así como escenarios transfronterizos complican aún más los retos tecnológicos y los requisitos de protección respectivos.

El sector salud de los Estados Miembros se ha conformado como una infraestructura de información crítica que debe hacer frente a los desafíos y los riesgos de las TIC.

4. La Estrategia Europea de Ciberseguridad: antecedentes y líneas de acción.

La Estrategia Europea de Ciberseguridad actúa como el marco teórico que guía las operaciones encaminadas a prevenir y neutralizar las amenazas y riesgos procedentes del ciberespacio. Dada su importancia, esta debe estar correctamente adaptada al contexto en el que actúa y, ha de tener a su disposición los medios y los presupuestos adecuados para una correcta consecución de sus objetivos.

Sin embargo, la realidad no es así, en tanto, el análisis del documento pone sobre la mesa una situación crítica: en primer lugar, existe una definición inadecuada de los riesgos y amenazas que emanan del ciberespacio; en segundo lugar, las líneas de acción de la Estrategia tienen objetivos demasiados difusos; en tercer lugar, las operaciones están enfocadas al corto plazo; en cuarto lugar, la dotación presupuestaria es escasa; en quinto y último lugar, no existen mecanismos de rendición de cuentas. Todos estos síntomas, que analizaremos más adelante, ponen de relieve que la ausencia de eficacia y eficiencia en la Estrategia de Ciberseguridad Europea es un problema real.

4.1 Antecedentes.

Antes de comenzar a analizar la Estrategia de Ciberseguridad Europea[26] de 2003, consideramos importante comentar brevemente sus antecedentes y el contexto donde se inserta: La Estrategia de Ciberseguridad Europea surge dentro de un marco de acciones encaminadas a solventar y mejorar el espacio en la red. El documento nace arropado por una serie de órganos, instituciones y políticas que ya estaban trabajando en torno a las diversas dimensiones de la seguridad desde finales de 1990.

En 2003, inspirándose la denominada Política Común de Seguridad y Defensa (PCSD) de 1999, se aprueba la Estrategia Europea de Seguridad. Las principales amenazas a las que el documento hacía referencia eran el terrorismo, la proliferación de armas de destrucción masiva, los conflictos regionales, la descomposición del Estado-Nación y la delincuencia organizada. Sorprendentemente, a pesar de la mirada amplia y multidimensional del documento, la Estrategia no incluía ninguna cuestión en torno a la ciberseguridad.

Un año más tarde, en 2004, la UE crea la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) tras ser consciente de que la ciberseguridad era uno de los temas principales en el imaginario europeo. La creación de la ENISA marca un hito en este compromiso con la nueva ciberrealidad ya no solo porque se constituye como la agencia de ciberseguridad que asesora a la Comisión y a los Estados Miembros, sino porque impulsó la creación del Programa Europeo para la Protección de Infraestructuras Críticas en 2007.

Teniendo en cuenta estas novedades, en el año 2008, el Informe sobre la aplicación de la Estrategia Europea de Seguridad pasa a incluir a la ciberseguridad como una amenaza más

[26] *The Cybersecurity Strategy of the European Union. An Open, Safe and Secure Cyberspace*, en: https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

a la que la UE deberá de hacer frente en un futuro cercano. Es en ese momento cuando se comienza a diseñar el programa "European Public-Private for Resilience" (EP3R), el cual saldrá a la luz en el año 2009.

Ahora bien, no es hasta 2010 con la aprobación de Estrategia de Seguridad Interior, cuando la ciberseguridad aparece de forma oficial como uno de los mayores desafíos comunes para toda Europa. Este documento marca un punto de inflexión en lo que a la cuestión de ciberseguridad se refiere al incluir a la ciberdelincuencia como una de las amenazas principales a las que debía enfrentarse Europa.

A partir de ahí, la conciencia en torno a la necesidad de proteger la dimensión virtual aumentó progresivamente hasta llegar a conformar en 2013 la actual Estrategia Europea de Ciberseguridad. En este sentido, cabe añadir que antes de la creación de la citada Estrategia Europea de Ciberseguridad, la UE creó en 2010 la "Digital Agenda for Europe". Ésta establece las hojas de ciber-ruta de la Unión y opera en siete campos sobre los que sostiene su acción global: el mercado digital en todos sus espectros, la interoperabilidad y los estándares en tanto construyen la democracia digital, la seguridad en el ciberespacio, la velocidad de los accesos a internet, la investigación y la innovación en las TIC, el acceso e inclusión para toda la población y lo digital como beneficio social de la propia UE. Y es desde ese tercer campo, la seguridad en internet, desde donde podemos enlazar con la Estrategia Europea de Ciberseguridad de 2013, la cual pasamos a analizar en profundidad.

4.2 La Estrategia Europea de Ciberseguridad y sus líneas de acción.

El 7 de febrero de 2013 se aprueba el texto de la Estrategia de Ciberseguridad Europea en un comunicado conjunto del Parlamento Europeo, el Consejo, el Comité Europeo de Asuntos Económicos y Sociales, y el Comité de las Regiones. El subtítulo "An Open, Safe and Secure Cyberspace"[27] nos permite centrar el objetivo principal de esta Estrategia: conseguir un ciberespacio abierto, protegido y seguro para todos los usuarios europeos. Por consiguiente, la Estrategia marca una serie de prioridades, en concreto, cinco campos de acción desde donde trabajar para conseguir este ciberespacio seguro, libre y abierto:

- La primera línea de acción tiene su foco de atención centrado en cómo incrementar las capacidades de ciberresiliencia. Es importante comprender que la mentalidad de fortaleza no funciona en el ciberespacio ya que ese se caracteriza por ser una dimensión de carácter abstracto, vaporoso y rizomático. internet es un escenario de conflicto donde desaparece la posibilidad de protegerse detrás de una línea Maginot o línea defensiva. Por dicha razón, desarrollar medidas que favorezca la capacidad de reacción y adaptación a los ataques externos es fundamental: "Internet is important: for our economy, for our values, and for our human rights. We all recognise that insecure systems could harm those benefits. And we recognise that we need to work together, within the EU and internationally, to achieve a safe and free internet. So our strategy is accompanied by a proposed directive to strengthen cyber-resilience within our single market".[28]

- La segunda línea de acción pretende reducir el cibercrimen. Unas de las acciones en las que esta segunda línea se ve materializada es en la creación en enero de 2013 del

[27] *The Cybersecurity Strategy of the European Union. An Open, Safe and Secure Cyberspace*, en: https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[28] Kroes Neelie (2013: "Using cybersecurity to promote European values", en: http://europa.eu/rapid/press-release_SPEECH-13-104_en.htm

Centro de Cibercrimen Europeo. Este, en colaboración con EUROPOL, actúa como una plataforma de alerta que permite aumentar los canales de información para luchar y prevenir la delincuencia en la red.

- La tercera línea de acción impulsa a trabajar en una política común de ciberdefensa, en coordinación con los objetivos de la Política Común de Seguridad y Defensa (PCSD). En este sentido, junto con ENISA, se han celebrado desde 2010 una serie de ejercicios de ciberseguridad, a modo de simulacro, que permiten comprobar la validez del sistema de defensa en la red.

- La cuarta línea de acción, que es la que más atención recibe en este momento, ya que se encarga de trabajar en la consecución de un mercado digital único. El desarrollo de los recursos industriales y tecnológicos necesarios en materia de ciberseguridad requieren de un mercado único que sea avalado por las instituciones europeas.

- La quinta línea de acción se encuentra vinculada a la consecución de una política común del ciberespacio, que busca el establecimiento de una política internacional y coherente con la promoción de los llamados valores europeos esenciales, promoviendo la democracia como mecanismo político que posibilita la igualdad.

5. Revisión crítica y vulnerabilidades relevantes en la ciberseguridad europea.

Tras analizar las líneas de acción de la Estrategia, es aconsejable llevar a cabo una evaluación de las realizaciones o avances que la Unión Europea ha realizado a lo largo de los últimos años en el campo de seguridad virtual.

5.1 Primera etapa: el decalaje.

Si repasamos la historia reciente de la Unión Europea, no se entiende que los Estados Miembros esperasen a la publicación del Informe sobre la aplicación de la Estrategia Europea de Seguridad[29] en 2008 para introducir la ciberseguridad en un documento estratégico de peso, cuando, ya en el año 2001 la ausencia de seguridad en el mundo virtual era un problema de primer nivel a escala internacional:

Cinco días después de los ataques a las Torres Gemelas, Estados Unidos tomó conciencia del papel que estaba jugando el ciberespacio en la extensión del fenómeno terrorista de carácter religioso. La utilización de servicios de mensajería electrónica encriptados, sumado al uso de cibercafés como plataformas de intercambio de información para terroristas, hizo que el gobierno americano reaccionase como nunca hasta entonces se había hecho: "La Administración estadounidense quiere intentar mantener a salvo internet de los ciberterroristas. El FBI ha lanzado una alerta contra el terrorismo cibernético, y el Senado norteamericano ha aprobado una serie de medidas que dan más facilidades a la policía para pinchar internet".[30]

Por el contrario, al otro lado del océano atlántico, la reacción de cara a la incertidumbre procedente del ciberespacio fue la nada. A pesar de que la UE elaboró su Estrategia de Seguridad dos años después del 11S, los Estados Miembros decidieron hacer

[29] *Informe sobre la aplicación de la Estrategia Europea de Seguridad*, en http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/ES/reports/104637.pdf
[30] Delclós, Tomás: "A la caza del ciberterrorismo", *El País*, 17 de septiembre de 2001, en: http://elpais.com/diario/2001/09/17/internacional/1000677638_850215.html

caso omiso a las advertencias americanas y no abordar el tema de los ciberataques en el documento estratégico de 2003. Desde su perspectiva, los desafíos procedentes del mundo virtual no representaban una amenaza de primer nivel a pesar de que durante ese mismo año Reino Unido fue objeto de casi 6000 ciberataques provenientes de Egipto, Pakistán, Marruecos y Turquía[31].

Los hechos acontecidos en Reino Unido sumados a los daños producidos por el ciberataque *SQL Slammer*[32] en Corea del Sur, Tailandia, Japón e India hacen incomprensible que la UE decidiese esperar al año 2008 para introducir a la ciberseguridad dentro de su apartado de amenazas a la seguridad comunitaria.

La conclusión que se puede extraer de esta primera etapa es que la UE empieza retrasada en el campo de la ciberseguridad al no incluir las amenazas virtuales en su Estrategia en el momento en el que tenía que haberlo hecho. El decalaje producido afectará, como veremos a continuación, a la gestión que se ha hecho de la ciberseguridad hasta los días presentes.

5.2 Segunda etapa: la oportunidad perdida.

El citado Informe sobre la aplicación de la Estrategia Europea de Seguridad[33], publicado en Bruselas el 11 de diciembre de 2008, pretendía ser una revisión de la aplicación de la ya analizada Estrategia Europea de Seguridad de 2003. Su misión era actualizar la Estrategia al nuevo contexto securitario de aquel momento. Dentro de esa ingente tarea aparecía la necesidad de incluir a la ciberseguridad dentro de la agenda europea como uno de los retos principales a los que los Estados Miembros debían hacer frente.

Dicho objetivo se cumplió en términos formales, pero no en términos reales, pues a pesar de que la dimensión virtual, ciertamente, pasó a incluirse en la lista de amenazas, la atención que se le prestó en términos reales fue meramente testimonial.

Este hecho, sumado a las marcadas limitaciones de la Estrategia -entiende que la seguridad es precondición para el desarrollo cuando es recíproco; confunde amenazas y riesgos; no propone conclusiones eficaces- hizo que el documento no alcanzara sus objetivos. Tal y como se argumentó en su momento, el Informe sobre la aplicación de la Estrategia Europea de Seguridad, no permitió que la Unión se dotara de los instrumentos adecuados para hacer frente a los nuevos riesgos y amenazas:

> "Resulta difícil identificar la naturaleza del Informe porque no se trata de una actualización del anterior como se esperaba, ni de una evaluación crítica de los resultados de la EES tras cinco años, ni de una declaración formal en la que se propongan nuevas líneas de acción al respecto [...] se prodigan lugares comunes y buenos deseos sin mayor voluntad de transcendencia […] el Informe tampoco revela nada sobre su finalidad, su lógica o sus consecuencias para la EES, parece

[31] Ranstorp, Magnus: "Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información", en Reinares, Fernando y Elorza, Antonio (eds.) (2004): *El nuevo terrorismo islamista. Del 11-S al 11*-M, Madrid, Ediciones Temas de hoy, S.A., pp. 201-222.
[32] BBC: "Virus-like attack hits web traffic" *BBC*. 25 enero 2003, en http://news.bbc.co.uk/2/hi/technology/2693925.stm
[33] *Informe sobre la aplicación de la Estrategia Europea de Seguridad*, en http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/ES/reports/104637.pdf

que su propósito real no es otro que el de engrosar el balance de la Presidencia aunque sea a costa de sumir a la PESD en un limbo estratégico"[34]

5.3 Tercera etapa: avances y retrocesos.

Esta tercera etapa, que se enmarca en el año 2013, se encuentra marcada por la publicación de dos documentos que pudieron ser pero que no fueron: la Estrategia de Ciberseguridad Europea y el documento Towards a European Global Strategy[35], elaborado por diferentes centros de estudio de Italia, Polonia, España y Suecia con la perspectiva de 2030.

Por un lado, el crecimiento exponencial del problema en el contexto internacional hizo necesaria la construcción de un nuevo documento centrado exclusivamente en la cuestión de la seguridad en internet: la Estrategia de Ciberseguridad Europea. La creación de este documento en 2013 tenía que haber intentado introducir una mejora considerable en la seguridad y operatividad del espacio virtual europeo. Sin embargo, el documento no fue elaborado de forma adecuada ya que carece de un enfoque a largo plazo, Teniendo en mente que la metamorfosis que sufre el ciberespacio es un proceso en constante ebullición que provoca que las amenazas a las que queremos hacer frente se hagan más sofisticadas en solo cuestión de segundos, la adopción de un enfoque cortoplacista en la Estrategia de Ciberseguridad no es la opción adecuada.

Otros ámbitos en los que se observan las diversas lagunas o vulnerabilidades de la Estrategia son la ausencia de mecanismos de rendición de cuentas o accountability y una dotación presupuestaria insuficiente.

- Ausencia de rendición de cuentas: Uno de los primeros síntomas que se pueden observar en el documento europeo de 2013 es que no existe una rendición de cuentas clara que obligue a los responsables de los ciberataques a pagar por los daños ocasionados. Esta ausencia de rendición de cuentas provoca que cuando se sufre el impacto de un ciberataque no se puedan exigir responsabilidades, pagos de seguros etc. Esto provoca, a su vez, que no exista una colaboración público-privada estable y efectiva, si no están claras las responsabilidades o, las que existen, se encuentran excesivamente fragmentadas, y que las empresas del sector privado no encuentren incentivos para establecer colaboraciones con el sector público. En este sentido, hemos de llegar a comprender que la ausencia de una colaboración público-privada en temas de ciberseguridad es un elemento extremadamente dañino y real que retrasa el desarrollo cibernético de la UE.

- Inexistencia de una dotación presupuestaria suficiente: Otro de los síntomas problemáticos que se pueden identificar tras analizar la Estrategia de Ciberseguridad Europea es que no existe un apartado que deje de forma clara cuál es la dotación presupuestaria que debe destinarse a las labores de prevención y resolución de conflictos en el ciberespacio. Por lo tanto, podríamos decir que en la Estrategia de Ciberseguridad Europea, al igual que ocurre en la española, no se informa a los

[34] Arteaga, Félix: "La Estrategia Europea de Seguridad, cinco años después", *Real Instituto Elcano,* 22 de enero de 2009, en http://www.realinstitutoelcano.org/wps/portal/rielcano/Imprimir?WCM_GLOBAL_CONTEXT=/elcano/Elcano_es/Zonas_es/ARI15-2009

[35] *Towards a European Global Strategy. Securing European influence in a changing world,* en http://www.realinstitutoelcano.org/wps/wcm/connect/4c2675804fc8b86b80b5caccba746acc/EGS_Report.pdf?MOD=AJPERES&CACHEID=4c2675804fc8b86b80b5caccba746acc

> ciudadanos ni a las empresas de cuál deben ser los recursos monetarios que se deben destinar al desarrollo de nuevas tecnologías digitales.

Respecto al segundo documento al que hacíamos referencia al principio del apartado, el Towards a European Global Strategy, cabe apuntar que este vio la luz gracias al interés que tuvieron los Ministerios de Asuntos Exteriores de Italia, Polonia, España y Suecia en llevar a cabo una reflexión sobre los retos a los que tendría que enfrentarse la Unión Europea en un futuro cercano (2030).

Este documento, producto de la reflexión de diferentes instituciones de prestigio, advierte que la Unión Europea tiene retos securitarios, económicos y sociales a escala local, regional y global. Así, los desafíos, que no amenazas, a las que la UE debe hacer frente son la agresión armada, los estados fallidos, los conflictos regionales, el terrorismo, las armas de destrucción masiva, el crimen organizado y los riesgos naturales, pero no la ciberseguridad. Se limita a decir lo siguiente:

> "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"[36]

Por lo tanto, a pesar de que el documento hace referencia a la problemática virtual cuando habla de la necesidad de garantizar el libre flujo de personas, capitales e información, el texto no incluye los ciberataques dentro de la lista de desafíos a los que la UE debe enfrentarse. De este modo, la idea que subyace en el documento Towards a European Global Strategy es que, a pesar de que sus autores son conscientes de que el ciberespacio es una dimensión estratégica clave para el futuro de la UE, estos consideran que las amenazas procedentes de este escenario de conflicto no son lo suficientemente potentes o urgentes como para incluirlas dentro de la agenda.

En conclusión, esta tercera etapa se cierra con avances y retrocesos coexistiendo al mismo tiempo. Se elabora una estrategia para cubrir el vacío técnico y legal en el que se encontraba sumido el ciberespacio, pero posteriormente los ciberataques no se introducen en los documentos estratégicos de peso.

5.4 Cuarta etapa: papel mojado.

La creciente complejidad del contexto internacional a consecuencia del terrorismo de Daesh, la crisis de refugiados y la inestabilidad económica, entre otros factores, ha obligado a la Unión Europea a replantarse sus intereses y estrategias securitarias tanto en el plano físico como en el plano virtual. El problema está en que la publicación de la European Union Global Strategy[37] en junio de 2016 no responde apropiadamente a las amenazas que emergen del ciberespacio.

---

[36] *Towards a European Global Strategy. Securing European influence in a changing world,* en http://www.realinstitutoelcano.org/wps/wcm/connect/4c2675804fc8b86b80b5caccba746acc/EGS_Report.pdf?MOD=AJPERES&CACHEID=4c2675804fc8b86b80b5caccba746acc

[37] *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy,* en https://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf pp. 21

Esta Estrategia, que se suponía iba marcar un cambio de paradigma en la seguridad de los Estados Miembros, atiende de forma confusa y mediocre la cuestión de la seguridad en internet. A pesar de ser cierto que sitúa la cuestión "ciber" como una de las prioridades de cara a garantizar la seguridad de la Unión en el futuro, el tratamiento que le otorga es muy similar al de etapas anteriores, es decir, frio y ausente de contenido. Ni resuelve el problema de las vulnerabilidades a nivel virtual ni aporta ningún avance en relación a los instrumentos y capacidades.

Todo ello hace que la Estrategia vuelva a ser un documento fallido en lo que a la ciberseguridad se refiere. No obstante, como veremos a continuación, acaba de publicarse un documento que inicia una quinta etapa en la que quizá sí se empiezan a solucionar las vulnerabilidades inherentes al ciberespacio desde hace más de una década.

5.5 Quinta etapa: una ventana de oportunidad.

Para solucionar los problemas heredados de etapas anteriores, el 6 de julio de 2016 el Parlamento Europeo publicaba una Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[38]. Este documento contiene aportaciones sumamente interesantes para la cuestión objeto de estudio ya que lleva a cabo una especie de autocrítica en la que reconoce que "las capacidades existentes no bastan para garantizar un elevado nivel de seguridad de las redes y sistemas de información en la Unión. Los niveles de preparación de los Estados miembros son muy distintos, lo que ha dado lugar a planteamientos fragmentados en la Unión"[39]

El documento marca así un punto de inflexión en el tratamiento de la ciberseguridad a nivel europeo al poner por primera vez una verdadera y especial atención en las vulnerabilidades existentes. Advierte que "la magnitud, la frecuencia y los efectos de los incidentes de seguridad se están incrementando y representan una grave amenaza para el funcionamiento de las redes y sistemas de información"[40] por lo que se pone como objetivo la creación de un plan que permita elaborar una respuesta efectiva y real contra la inseguridad en la red.

La Directiva apunta que esa respuesta deberá tener como pilares principales el establecimiento de "mínimos comunes en materia de desarrollo de capacidades y planificación"[41], la potenciación del intercambio de información con los operadores de servicio, la consolidación del mercado interior digital y la mejora de la protección de las infraestructuras críticas.

Todas estas novedades permiten afirmar que esta Directiva, elemento central de esta quinta etapa, es el documento que la UE había estado esperando desde hace años. El texto cumple su objetivo y se constituye como una ventana de oportunidad como no había existido antes en el ámbito europeo. Sólo cabe esperar que las medidas diseñadas y las propuestas elaboradas pasen del papel a la realidad y no queden aplazadas o guardadas en un cajón de un despacho de Bruselas como ya ha ocurrido antes en numerosas ocasiones con la cuestión de la ciberseguridad.

---

[38] *Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*, en https://www.boe.es/doue/2016/194/L00001-00030.pdf

[39] *Ibíd.*

[40] *Ibíd.*

[41] *Ibíd.*

6. Conclusiones.

El análisis desarrollado en este capítulo nos permite comprender que el ciberespacio es un escenario de conflicto altamente complejo al estar en constante evolución. La realidad nos ha demostrado que la combinación de ciberataques con ataques físicos tradicionales puede ser la fórmula perfecta para paralizar al completo las infraestructuras críticas de un país[42]. Los ejemplos del virus Stuxnet, el virus Flame o los (ciber)enfrentamientos entre Estonia y Rusia ponen de relieve que los ciberataques son armas sumamente dañinas y eficaces ya que requieren pocos recursos en comparación con su prácticamente ilimitada capacidad de destrucción.

Ni la Unión Europea ni ningún otro actor del panorama internacional se encuentra a salvo de las amenazas procedentes del ciberespacio. Por lo tanto, si sabemos que los actuales ciberataques ya no sólo tienen el mismo efecto destructivo que una bomba, sino que también pueden llegar a tomar el control de los objetivos a los que atacan, hemos de conseguir desarrollar los mecanismos que permitan a la Unión Europea constituir un ciberespacio verdaderamente seguro, flexible y operativo.

Partiendo de la base de que la gestión del ciberespacio por parte de la Unión Europea no ha sido la adecuada desde un primer momento, es urgente que los Estados Miembros reaccionen y hagan realidad lo planteado en los documentos oficiales:

En primer lugar, para construir una Unión Europea resiliente a nivel cibernético es necesario construir mecanismos de rendición de cuentas que permitan garantizar un uso protegido de internet.

En segundo lugar, con el objetivo de proteger las infraestructuras críticas, la Unión Europea debe fomentar una colaboración público-privada que permita desarrollar mayores y mejores recursos industriales de carácter digital. La firma de contratos de asociación público-privada (PPP) en materia de ciberseguridad es la llave para diseñar un verdadero mercado único digital a nivel europeo. La coordinación de respuestas con socios públicos y privados es la única forma de construir un ciberespacio basado en la confianza, la seguridad y la transparencia.

En tercer lugar, la Unión Europea debe potenciar el intercambio de información con otros actores internacionales. Sólo así la Unión Europea podrá proteger el ciberespacio sin dañar los derechos y libertades fundamentales de sus usuarios. En este sentido, su colaboración bilateral con Estados Unidos en temas de ciberseguridad y ciberdelincuencia, así como su colaboración con la OTAN en tareas de defensa cibernética son elementos cruciales que se deben potenciar y expandir en el futuro.

En cuarto lugar, la Unión Europea tiene que diseñar mecanismos de alerta temprana en el ciberespacio con el objetivo de poder prevenir futuras vulnerabilidades y advertir futuros ciberataques. En este sentido, la Unión Europea no debe escatimar en presupuestos ya que el diseño de cortafuegos digitales o la creación de equipos de defensa cibernética de reacción rápida puede suponer la diferencia entre una Europa segura virtualmente o una Europa desmembrada por los ciberataques.

[42] Innerarity, Daniel (2013): *Un mundo de todos y de nadie. Piratas, riesgos y redes en el nuevo desorden global*, Barcelona, Espasa Libros.

En quinto lugar, la Unión Europea debe entender que la única forma de garantizar un elevado nivel de seguridad en sus redes y sistemas de información es a través de la adopción de estrategias proactivas enfocadas al largo plazo. Si los ciberataques son amenazas securitarias en constante evolución que hacen que los mecanismos de seguridad virtuales más potentes se vuelvan inefectivos en cuestión de segundos, las estrategias de ciberseguridad europeas deben tener un enfoque preventivo en lugar de reactivo.

En definitiva, los pasos dados desde la UE en el mundo de la ciberseguridad no son en absoluto suficientes. Europa necesita que su Estrategia de Ciberseguridad sea realmente capaz de integrar a las diferentes Estrategias nacionales. Es urgente una mayor determinación, unos mayores recursos y unos mejores instrumentos que permitan a la Unión implementar una gestión de crisis y una prevención de ciberconflictos verdaderamente eficaz. Para que la Unión Europea gestione la ciberseguridad de forma eficaz y eficiente deberá no solo subsanar las vulnerabilidades presentadas, sino también hacer efectivas todo el conjunto de reformas que ha ido aplazando injustificadamente desde 2003. Hasta que todo eso no se haga realidad, la Unión Europea y sus ciudadanos seguirán yendo a la deriva en el ciberespacio y, en esta situación, los únicos beneficiados son los piratas electrónicos, los ciberterroristas y los cibercriminales.

Bibliografía Seleccionada

Arteaga, Félix: "La Estrategia Europea de Seguridad, cinco años después", *Real Instituto Elcano,* 22 de enero de 2009, en http://www.realinstitutoelcano.org/wps/portal/rielcano/Imprimir?WCM_GLOBAL_CONTEXT=/elcano/Elcano_es/Zonas_es/ARI15-2009

Bulnes, Ana: "Más allá de Anonymous: censo de grupos hacktivistas" *Silicon*, 28 de junio de 2011, en http://www.silicon.es/mas-alla-de-anonymous-censo-de-grupos-hacktivistas-2196485#4ivLHhMoWFCZz82b.99

Center for Strategic and International Studies (CSIS).(n.d) :"Biometrics and Security" en https://www.csis.org/programs/strategic-technologies-program/cybersecurity/other-projects-cybersecurity/biometrics-and

Comisión Europea (2013): "Los puertos marítimos de Europa en el horizonte de 2030: retos futuros". Bruselas, 23 de mayo de 2013, en http://europa.eu/rapid/press-release_MEMO-13-448_es.htm

"Conclusiones del Consejo sobre la comunicación conjunta de la Comisión y de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, titulada "Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro". nº 12109/13, en http://register.consilium.europa.eu/doc/srv?f=ST+12109+2013+INIT&l=es

Conde Vilda, C et al (2007); "Biometría facial en el aeropuerto de Barajas". *Perspectiva Empresarial.* ed. Universidad Rey Juan Carlos, nº9, abril 2007.
"Consumerisation: The Power of Many", *Economist*, 8 October 2011, en http://www.economist.com/node/21530921

Diaz Gómez, Andrés (2010):"El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest", *REDUR 8*, Diciembre 2010.
Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, en https://www.boe.es/doue/2016/194/L00001-00030.pdf

ENISA (2011):"Cyber Security Aspects in the Maritime Sector" en https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

ENISA (2015): "Secure Use of Cloud Computing in the Finance Sector" en https://www.enisa.europa.eu/publications/cloud-in-finance

Gómez, Ángel (2012): "El ciberespacio como escenario de conflicto. Identificación de las amenazas", en *El ciberespacio. Nuevo escenario de confrontación*, Madrid, Ed. Ministerio de Defensa

Hurtaud, S (2014):"Cyber security Time for a new paradigm". *Information & Technology Risk*. Ed. Deloitte.

Informe sobre la aplicación de la Estrategia Europea de Seguridad, en http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/ES/reports/104637.pdf

Innerarity, Daniel (2013): *Un mundo de todos y de nadie. Piratas, riesgos y redes en el nuevo desorden global*, Barcelona, Espasa Libros.
Kroes Neelie (2013:"Using cybersecurity to promote European values", en: http://europa.eu/rapid/press-release_SPEECH-13-104_en.htm

Kurbalija, J; Gelbstein, E.(2005):"Gobernanza de Internet: Asuntos, Actores y Brechas", Ed. DiploFoundation, pág 82 en http://textus.diplomacy.edu/textusbin/env/scripts/Pool/GetBin.asp?IDPool=1090

Lynn, William J.: "Defending a new domain: The Pentagon's cyberstrategy" *Foreign Affairs* , vol.89, nº.5 (September-October 2010).

Martin R, Stytz.; Sheila B. Bank (2014): "Cyber Warfare Simulation to Prepare to Control Cyber Space". *National Cybersecurity Institute Journal*, vol 1, nº2.

Ranstorp, Magnus: "Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información", en Reinares, Fernando y Elorza, Antonio (eds.) (2004): *El nuevo terrorismo islamista. Del 11-S al 11*-M, Madrid, Ediciones Temas de hoy.

Robinson, N.(2014): "EU cyber-defence: a work in progress". *EU Institute for Security Studies*, vol.10, marzo 2014, en http://www.iss.europa.eu/uploads/media/Brief_10_Cyber_defence.pdf

Sanger, David and Perloroth, Nicole: "Bank Hackers Steal Millions via Malware", *New York Times*, 14 February 2015, en http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=1

Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy, en https://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf

Tapiador.Marino, Sigüenza.Juan Alberto (2005):" Tecnologías biométricas aplicadas a la seguridad", Madrid, ed. RA-MA.

The Cybersecurity Strategy of the European Union. An Open, Safe and Secure Cyberspace, en: https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

Torrecuadrada, Soledad (2013): "Internet y el uso de la fuerza", en *Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio,* Granada, Ed. Universidad de Granada.

Towards a European Global Strategy. *Securing European influence in a changing world,* en http://www.realinstitutoelcano.org/wps/wcm/connect/4c2675804fc8b86b80b5caccba746acc/EGS_Report.pdf?MOD=AJPERES&CACHEID=4c2675804fc8b86b80b5caccba746acc

Una Europa segura en un mundo mejor – Estrategia Europea de Seguridad 2003, Bruselas 12 de diciembre de 2003.en
https://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIES.pdf