LA CIBERDEFENSA Y SUS DIMENSIONES GLOBAL Y ESPECÍFICA EN LA ESTRATEGIA DE SEGURIDAD NACIONAL ESPAÑOLA

Autoras: *Cristina Amich Elías*[1]
Teniente Auditor. Doctora en Derecho.

Ana Pilar Velázquez Ortiz[2]
Capitán Auditor. Máster en Investigación en Ciencias Jurídicas.

Resumen

La Estrategia de Seguridad Nacional de 2013 incluye los ciberataques como una de las amenazas a las que España está expuesta y a las que, siguiendo las líneas de estrategia que se definen, habrá que hacer frente. Sin embargo, el estudio de las ciberamenazas no puede realizarse de forma aislada respecto de otras que, asimismo, son identificadas por el citado documento. Antes al contrario, la práctica totalidad de las amenazas citadas por la ESN, pueden manifestarse a través de un ataque cibernético, de modo que resulta necesario abordar este tema desde una perspectiva global. De

[1] crisamich@gmail.com

[2] averlort@gmail.com

este análisis surge la necesidad de plantear en qué momento un ciberataque deja de ser una amenaza para la seguridad y comienza a serlo para la Defensa Nacional. Únicamente un enfoque jurídico que permita discernir en qué ocasiones un ciberataque puede ser considerado uso de la fuerza, podrá dar respuesta a esta cuestión.

Palabras clave: Estrategia de Seguridad Nacional; ciberamenazas; Defensa Nacional; uso de la fuerza.

Cyberdefense and its global and specific dimensions in the Spanish National Security Strategy.

Abstract:

The 2013 Spanish National Security Strategy includes cyberattacks as one of the threats which Spain is exposed to, and which according to the defined strategy routes, Spain will have to face to. Nevertheless, cyberthreats analysis cannot be done disconnectedly from those threats which are, also included in the document. On the opposite, most part of the threats mentioned in the ESN, are able to turn up through a cyberattack, so a global perspective, analyzing the subject, is due. A new question arises from this analysis, in the sense of having in mind when a ciberattack becomes a threat for Defense instead of a threat for security. A legal perspective will be the only proper way to settle when a cyberattack could be considered as a use of force, in order to answer the former question.

Key words: Spanish National Security Strategy; cyberthreats; Defense; use of force.

Recibido: 07-04-2014
Aceptado: 03-06-2014

1. INTRODUCCIÓN

El presente artículo se propone abordar el estudio de los ciberataques en la medida en que éstos constituyen una de las amenazas expresadas en la Estrategia de Seguridad Nacional (en adelante, ESN). En un primer momento dicho estudio analizará el fenómeno de las ciberamenazas desde una perspectiva global, por entender que, para responder al impacto de éstas sobre la seguridad nacional resulta necesario abordarlas desde un concepto amplio e integrado.

Así, la ESN hace mención expresa a la capacidad potenciadora de las nuevas tecnologías en el análisis de otros riesgos como los conflictos armados, el

terrorismo, el espionaje y la seguridad de las infraestructuras críticas, poniendo un especial énfasis en las posibilidades resultantes de las mismas de las que pueden proveerse los grupos terroristas o que pueden originar actividades de espionaje. Pero, se debe tener en cuenta que, además, la facilidad de acceso a estas nuevas tecnologías, su universalización, su continuo desarrollo hacia posibilidades de uso que incrementan nuestra dependencia como Estado y sociedad de las mismas, ponen de relieve la necesidad de una concienciación y formación también universales, no sólo sobre los potenciales peligros y amenazas que a través de la red pueden sufrirse, sino sobre el desarrollo y empleo de la multiplicidad de capacidades y ventajas por parte de todos los posibles actores implicados, con el objeto de poder conseguir una verdadera seguridad nacional a través de una defensa profunda.

Señalado esto y, teniendo en cuenta que, desde una perspectiva más específica, la dimensión virtual es además un elemento concreto del conflicto armado, que afecta a conceptos de guerra como estado neutral o personal combatiente, resulta preciso igualmente, analizar hasta qué punto, no ya la Seguridad, sino la Defensa Nacional, puede verse comprometida por las ciberamenazas, y más concretamente, por ataques de naturaleza cibernética.

En consecuencia, se estudiará qué papel juega el recién creado Mando Conjunto de Ciberdefensa y en qué supuestos los ataques informáticos conllevarán la posibilidad de que dicho Mando active una respuesta. Así, desde el punto de vista jurídico, la principal tarea consistirá en discernir qué ataques resultan irrelevantes para la Defensa Nacional, en contraposición a aquéllos que pueden suponer un uso de la fuerza y por lo tanto, una repuesta en consecuencia. Toda vez que dichos actos no resultan, a priori, completamente asimilables al tradicional concepto de uso de la fuerza, se hace preciso examinar las principales teorías *iusinternacionalistas*, a la luz de los supuestos recientemente constatados.

2. LA DIMENSIÓN GLOBAL DE LA CIBERDEFENSA EN LA ESTRATEGIA NACIONAL DE SEGURIDAD

En nuestro presente y nuestro relativamente conocido futuro, ¿resulta adecuado separar los conceptos de seguridad y ciberseguridad? ¿Es posible mantener las ciberamenazas como un riesgo específico con características propias, y sólo relativamente vinculado al resto de los riesgos? ¿Es la ciberseguridad un elemento de la seguridad o debemos caminar hacia una concienciación de que la seguridad y la ciberseguridad se han convertido, de hecho, en una única cosa?

A lo largo de los últimos años se ha producido una importante concienciación de las dimensiones, ventajas y peligros de las nuevas tecnologías en el ámbito de la seguridad nacional. Ello ha llevado a la inclusión de las ciberamenazas como

un riesgo determinado y concretizado en la Estrategia de Seguridad Nacional (ESN) 2013[3].

Dicha Estrategia se presenta como un abordaje amplio e integral de la seguridad nacional la cual es concebida como un conjunto de ámbitos concernientes a la seguridad del Estado y de sus ciudadanos, que son variables según las rápidas evoluciones del entorno estratégico y abarcan desde la defensa del territorio a la estabilidad económica y financiera o la protección de las infraestructuras críticas.

La progresiva asunción de la necesidad de abordar la seguridad desde una perspectiva amplia e integradora, no centrada exclusivamente en riesgos militares y responsabilidades de protección vinculadas a la defensa, ha estado presente en los últimos años, no sólo en la primera Estrategia Española de Seguridad de 2011[4], sino en la propia Directiva de Defensa Nacional 1/2008[5], en la que ya se señalaba que a los tradicionales riesgos y amenazas a la seguridad, que implicaban una respuesta casi exclusivamente militar, se han unido otros que, aunque menos destructivos, degradan y dificultan el desarrollo social y económico de los países. En consecuencia, los problemas económicos y sociales constituyen también un motivo de preocupación para nuestra seguridad global.

Por ello, la Estrategia Española de Seguridad (EES) de 2011 introdujo claramente el concepto de enfoque integral, remarcando la necesidad *de integrar todas y cada una de las dimensiones de la seguridad, haciéndolas converger hacia objetivos comunes y conscientes de las múltiples relaciones que existen entre ellas*. Ello llevó a identificar una serie de "potenciadores de riesgo" como los "Desequilibrios demográficos", la "Pobreza y desigualdad" o los "Peligros tecnológicos", al tiempo que se incluían como amenazas y riesgos específicos elementos como la "Inseguridad económica y financiera", la "Vulnerabilidad energética", las "Ciberamenazas" y los "Flujos migratorios no controlados".

Al hablar concretamente de los peligros tecnológicos como "potenciadores de riesgo", la EES de 2011 señalaba que *la tecnología puede potenciar o crear nuevas amenazas y riesgos para la seguridad*. La frase, simple y directa, resume perfectamente la dimensión envolvente de la tecnología informática y sus dimensiones transversales. Sin embargo, la evidencia de dichas características se diluía posteriormente en el momento en que el peligro tecnológico se concretizaba en un ámbito, el ciberespacio, que si bien se definía como algo que *iba más allá de la Red, incluyendo dispositivos móviles como los teléfonos móviles, la televisión terrestre y las comunicaciones por satélite*, aparecía conceptuado como espacio determinado, diferente y, sobre todo, independiente del ámbito real o físico.

---

[3] *Estrategia de Seguridad Nacional. Un Proyecto Compartido*, Presidencia del Gobierno, 2013.

[4] *Estrategia Española de Seguridad. Una responsabilidad de todos*, Gobierno de España, 2011.

[5] Disponible en: http://www.defensa.gob.es/Galerias/politica/armamento-material/ficheros/DGM-directiva-defensa-nacional-1-2008.pdf

Siguiendo dicha conceptualización de espacio diferenciado, a la hora de abordar el riesgo de las ciberamenazas, la EES de 2011 hablaba de conseguir un ciberespacio seguro, y si bien en la consecución de dicho objetivo se tenían especialmente en cuenta factores globales y ciertas interdependencias destacadas entre mundo físico y mundo cibernético, el análisis del riesgo y las líneas de acción dibujadas se circunscribían exclusivamente al propio ámbito cibernético, sin que se realizasen referencias concretas al mismo en los análisis específicos del resto de los riesgos enumerados en la Estrategia.

En los dos últimos años, y en línea con la evolución conceptual que ha tenido lugar en los países de nuestro entorno, y con la evolución real de las posibilidades brindadas por la tecnología, España ha llevado a cabo una revisión de su estrategia de seguridad, al tiempo que, también en consonancia con las iniciativas de otros países, configuraba una novedosa Estrategia de Ciberseguridad Nacional[6].

La Estrategia Nacional de Seguridad de 2013 realiza un planteamiento convergente, ahondando en la visión integral en un mundo globalizado y cambiante. La Estrategia de 2013 se basa en los principios de unidad de acción, anticipación, prevención, eficiencia y sostenibilidad en el uso de los recursos, y resilencia y recuperación. Está estructurada en cinco capítulos a lo largo de los cuales se hace continuo hincapié en la visión integral y en lo que se ha venido en denominar, tal y como aparece en el propio título de la Estrategia, un "proyecto compartido", progresando así, al menos teóricamente, desde los antiguos conceptos de seguridad y defensa hacia una nueva perspectiva de seguridad global.

Este documento identifica, como se hacía en 2011, una serie de riesgos y amenazas, en un proceso de reconocimiento estratégico. Entre ellos se mantiene la inclusión de las ciberamenazas. Desaparecen de forma explícita los llamados potenciadores de riesgo que, aunque son nombrados de forma esporádica como factores que sin ser en sí mismos un riesgo o una amenaza, pueden desencadenarlos o agravarlos, no aparecen singular y explícitamente analizados. El reconocimiento del valor estratégico del entorno virtual, las nuevas tecnologías y en definitiva del ciberespacio en el ámbito de la seguridad nacional es sin duda un acierto y una necesidad, pero sigue pareciendo, en cierto modo, limitado, si tenemos en cuenta la vertiginosa evolución de las posibilidades tecnológicas y la cada vez mayor interdependencia entre espacio físico y ciberespacio.

La ESN reconoce dicha interdependencia en mayor medida que su documento predecesor y no duda en mencionar la transversalidad de éste y otros riegos específicos, pero aún deja al margen una visión concienciada de la verdadera

[6] La Estrategia de Ciberseguridad Nacional fue aprobada el pasado 5 de diciembre de 2013 por el Consejo de Seguridad Nacional y puede consultarse a través del siguiente enlace: www.lamoncloa.gob.es/ServiciosdePrensa/NotasPrensa/PG/2013/051213ConsejoSeguridadNacional.htm.

dimensión global de las nuevas tecnologías como factor no independiente, dadas las ventajas tácticas, competitivas, económicas, etc. que proporciona. Así, si bien las ciberamenazas pueden analizarse como un riesgo específico si las definimos, según la ESN, *como un potente instrumento de agresión contra particulares e instituciones públicas y privadas, ya sean en sus modalidades de ciberterrorismo, ciberdelito/cibercrimen, ciberespionaje o hacktivismo*, el concepto debe abordarse desde una perspectiva mucha más amplia, y su configuración como un elemento cada vez más presente e inseparable del resto de los riesgos no puede ser pasado por alto. Como señala la propia Estrategia, *el ciberespacio es un medio para la materialización de otros riesgos y amenazas,* pero, sobre todo, debemos llegar a la plena asunción de que el ciberespacio no es una realidad separada de la vida cotidiana, se ha convertido en la vida cotidiana.

Como venimos señalando, la ESN de 2013 no olvida la interdependencia y menciona la capacidad potenciadora de las nuevas tecnologías en el análisis de otros riesgos como los conflictos armados, el terrorismo, el espionaje y la seguridad de las infraestructuras críticas, resaltando especialmente las posibilidades que las mismas brindan a los grupos terroristas *para reclutar miembros, obtener recursos, ejecutar atentados y multiplicar el impacto de sus acciones*, o para realizar tareas de espionaje, y, fundamentalmente, su interrelación con las infraestructuras críticas y el soporte de los servicios públicos esenciales.

Consideramos, sin embargo, y como venimos repitiendo, que una visión que integre la dimensión virtual y las nuevas tecnologías en el concepto global de seguridad, más allá de una enumeración *agregadora* anteriormente citada, hubiese sido lo deseable a este respecto. No parece suficiente señalar que el ciberespacio puede convertirse en escenario de un conflicto armado o que los terroristas pueden aprovecharse de las nuevas tecnologías, es preciso una concienciación más plena de la globalidad de la ciberseguridad: la dimensión virtual es ya, de hecho, y como demuestran diversos sucesos reales de los últimos años, un elemento más del conflicto armado, no únicamente un posible escenario de conflicto, afectando a conceptos de guerra tan necesarios y clásicos como estado neutral o personal combatiente. El terrorismo, el crimen organizado, el espionaje, no sólo utilizan las nuevas tecnologías para incrementar su eficiencia, simplemente no pueden ya existir desvinculadas de éstas, del mismo modo que no puede hacerlo el resto de la sociedad, dependiente, ineludiblemente, en todas sus dimensiones, y el hacktivismo ha pasado a ser profesional y multimilitante, porque *technologies are not only become more powerful—they are also becoming more ubiquitous. We used to think that, somehow, digital technologies lived in a national reserve of some kind—first, we called this imaginary place "cyberspace" and then we switched to the more neutral label of "the Internet"—and it´s only in the last few years, with the proliferation of geolocational services, self-driving cars, smart glasses, that we grasped that, perhaps, such national reserves*

were a myth and digital technologies would literally be everywhere: in our fridges, in our belts, in our books, in our trash bins[7].

Todo ello implica que, al abordar la seguridad nacional, no es suficiente hablar de proteger el ciberespacio como un escenario independiente por sus posibles impactos en la realidad, sino de proteger la realidad en sus dimensiones física y virtual interrelacionadas, reconociendo la irremediable existencia de un mundo ya inseparable de la tecnología.

A pesar de que la Estrategia no muestra una completa asunción de esta concienciación de la ciberseguridad como un elemento global e inseparable del resto de las dimensiones, el reconocimiento de su valor estratégico se ha traducido también en la adopción de una Estrategia de Ciberseguridad Nacional[8], siguiendo igualmente las tendencias de nuestro entorno en este sentido, y en consonancia con las líneas marcadas tanto desde la OCDE[9] como de la UE[10].

Esta Estrategia se estructura igualmente en cinco capítulos, a lo largo de los cuales se pone de manifiesto la conciencia de los impactos trasversales de las nuevas tecnologías y sus peligros (y beneficios) en la sociedad española y en el funcionamiento del país, así como en su dimensión global y dinámica.

Desde nuestro punto de vista, dos cuestiones deben ser especialmente destacadas en este documento: la mención y desarrollo de la idea de responsabilidad compartida como principio rector de la Estrategia, y la inclusión de los Objetivos IV y V: "sensibilización de los ciudadanos, profesionales, empresas y Administraciones públicas de los riesgos derivados del ciberespacio" (IV) , y "Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad" (V).

Y ello debido a que el reconocimiento de la necesidad de la sensibilización o concienciación de la sociedad en su conjunto de los riesgos del ciberespacio parece indicar una autoconciencia de la globalidad de dichos riesgos, más allá de los límites virtuales, y de la necesidad de formación y educación para contar con las capacidades necesarias para hacer frente a los retos de dicha globalidad.

La historia reciente ha demostrado dicha dimensión global, y la ineludible e innegable implicación de una multiplicidad de actores públicos y privados en

---

[7] MOROZOV, E., "Smart", *what *should* we be worried about?,* Annual question 2013, http://edge.org/response-detail/23829. Acceso: 1 de abril de 2014.

[8] *Estrategia de Seguridad Nacional.*

[9] *Cybersecurity Policy Making as a turning point. Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy,* OECD, 2012. Disponible en: http://www.oecd-ilibrary.org/science-and-technology/cybersecurity-policy-making-at-a-turning-point_5k8zq92vdgtl-en. Acceso: 1 de abril de 2014.

[10] *Plan de ciberseguridad de la UE para proteger una red abierta plena de libertad y de oportunidades en línea*, Comisión Europea, 2013. Disponible en: http://europa.eu/rapid/press-release_IP-13-94_es.htm. Acceso: 25 de marzo de 2014.

las diversas facetas que pueden adoptar los riesgos cibernéticos. Así, mientras los sucesos de Estonia en el 2007 (ataques DDOS) reclamaron la atención sobre las limitaciones de las regulaciones nacionales en relación con los denominados *crossbordercrimes*, y la cada vez más acuciante necesidad de una cooperación internacional que aún está lejos de articularse adecuadamente, otros sucesos como los de Lituania en 2008 evidenciaron la facilidad de convertir un país en un *target* global, sin necesidad de un gran despliegue de medios de ataque, al tiempo que acontecimientos como los de Bielorrusia en 2008 indicaban la emergencia de otra importante faceta del peligro, esto es, el empleo de un concepto tergiversado de seguridad nacional, con el objetivo de legitimar el control sobre las libertades ciudadanas.

Este último punto es especialmente importante a la hora de analizar la transversalidad de las ciberamenazas, en el sentido de ampliar la definición proporcionada por la Estrategia de Seguridad Nacional antes mencionada, así como la específica relevancia de la sensibilización de todos los sectores en relación con la defensa de los intereses estratégicos del país. Sólo un conocimiento suficiente y fundamentado de la verdadera falta de límites del ciberespacio y sus implicaciones en el mundo real, puede llevar a la efectiva aplicación de una Estrategia de seguridad que no sólo pretenda la defensa y lucha frente y contra riesgos "externos" (ciberamenazas entendidas como *ataques*) sino que impida la degeneración del sistema democrático desde la propia articulación de medidas mal diseñadas en base a un concepto equívoco del riesgo cibernético.

Señalamos esto porque consideramos que sobredimensionar el ciberespacio como un riesgo específico, en vez de abordarlo como un componente de la realidad, y al margen de que se mencione de manera más o menos destacada la cara bondadosa de las nuevas tecnologías en los documentos mencionados, puede llevar también al fomento de una concienciación errónea de la sociedad en su conjunto en relación con este espacio, en el sentido de potenciar miedos no fundamentados a desarrollar una verdadera implicación, aprendizaje y uso de las posibilidades presentes y futuras del mundo informático.

Es decir, limitar la potencialidad de uso de las nuevas tecnologías, convirtiéndolas en un riesgo específico y destacado, puede derivar en un conocimiento compartimentado y limitado de las mismas por parte de todos los actores implicados lo que, a su vez, conlleva un doble peligro: por un lado, produce una dispersión de comprensión del impacto en la seguridad global de usos concretos y extendidos por parte de ciudadanos, administraciones, instituciones y empresa, usos considerados inofensivos, reduciendo el interés por fortalecer los mecanismos de protección en dichos ámbitos de habitualidad; por otro, produce el desconocimiento de posibilidades más amplias –e identificadas como terreno de unos pocos expertos (*cloud computing*, virtualización, realidad aumentada-) de empleo de dichas tecnologías para fortalecer al Estado en su conjunto.

Así, los usos considerados inofensivos se convierten en parte del riesgo global al impactar en aspectos como la estabilidad económica, al tiempo que el rechazo a conocer y emplear la multiplicidad de posibilidades impacta en el desarrollo estratégico y en la innovación, y deja desprotegido al país frente aquellos actores que sí han desarrollado un conocimiento bien cimentado sobre las posibilidades de las nuevas tecnologías y las interrelaciones con el mundo físico, siendo dicho conocimiento y no el ciberespacio en sí, o un ciberataque concretizado, lo que se debe considerar un riesgo específico de la seguridad nacional.

Por ello, resulta imprescindible combinar la ESN y la Estrategia de Ciberseguridad con la Agenda Digital para España[11], aprobada en 2013 por el Consejo de Ministros, en la que se establece, entre diversos objetivos, el de reforzar la confianza en el ámbito digital, y a partir de la cual se crea un Plan de Confianza Digital (2013-2015) que *hace suyo el mandato conjunto de la Agenda Digital para España, de la Estrategia Europea de Ciberseguridad y de la Estrategia de Seguridad Nacional para avanzar en los objetivos conjuntos de construir un clima de confianza que contribuya al desarrollo de la economía y la sociedad digital, disponer de un ciberespacio abierto, seguro y protegido, garantizar un uso seguro de las redes y los sistemas de información, y responder además a los compromisos internacionales en materia de ciberseguridad*[12]. Por tanto, y como venimos señalando, todas las facetas de las nuevas tecnologías, incluido el aprendizaje y fomento del uso de sus múltiples posibilidades, deben integrarse en una estrategia de seguridad, pues, el aislamiento ciudadano/empresarial/público ante los nuevos desarrollos, ya sea por miedo o desconocimiento, impacta en la potencialidad del país en su conjunto y en sus posibilidades de defensa.

En ese fomento de la confianza digital y del desarrollo tecnológico, no puede olvidarse el pilar fundamental que todo lo sustenta, nuestro sistema democrático, así, y como señala Haim Harari, *the only way to cope with the problem is to allow the structure of modern liberal democracy to evolve and adapt to the new technologies. That has not yet begun to happen. We do not yet have solutions and remedies, but there must be ways to preserve the basic features of democracy, while fine-tuning its detailed rules and patterns, so as to minimize the ill effects and to allow modern science and technology to do significantly more good than harm*[13].

Como Estado –tanto independiente como integrado en la Comunidad internacional – no podemos entender las ciberamenazas exclusivamente como ataques o disrupcciones más o menos concretizados y perpetrados por terroristas, espías, enemigos o hackers, ni siquiera como los riesgos de caída de la red de infraestructuras

[11] Disponible en: www.agendadigital.gob.es.

[12] http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-confianza-ambito-digital.aspx.

[13] HARARI, H., "Tecnology may endager democracy", *What *should* we be worried about?*, Annual question 2013, http://edge.org/response-detail/23835. Acceso: 1 de abril de 2014.

críticas por motivos humanos o naturales. La amenaza actual y futura a nuestra seguridad nacional derivada de las nuevas tecnologías es la falta de adaptación de nuestro sistema democrático a esa dimensión, ejemplificado en cuestiones como la falta de una normativa legal adecuada, el recurso a medidas administrativas que cercenan derechos para paliar peligros que no siempre son tales, la falta de inversión en medios y formación tecnológica, el empleo interesado de *big data*[14], el mantenimiento de conceptos clásicos de gestión corporativa y administrativa, etc.

Por ello, desde la perspectiva de la seguridad global no procede hablar únicamente de esas ciberamenazas específicas señaladas (ciberterrorismo, ciberespionaje, etc.) que, en definitiva, no son más que versiones modernas de clásicos peligros, sino que debemos centrarnos en las grandes áreas donde se centra el inmediato futuro de las amenazas: la ingeniería social (manipulación de formularios, llamadas no solicitadas, mensajes,…) y los ataques multivectoriales donde se combinan diferentes tipos de soporte (correo electrónico, mensajes en blogs, redes sociales, wikis,…., voz, vídeo, audio, etc.). Del mismo modo, no podemos olvidar que nos encontramos con la implantación creciente del Internet móvil y la consiguiente proliferación de dispositivos móviles (acceso mediante todo tipo de dispositivos, teléfonos inteligentes, tabletas tipo ipad, libros electrónicos, microordenadores *netbooks*, ordenadores think (tontos, con poca memoria y capacidad de proceso conectados a *la Nube*) videoconsolas, acceso desde todo tipo de medios de comunicación, automóviles, trenes, aviones, autobuses, barcos, …), de las tecnologías *cloud computing*, la virtualización, o el avance imparable de las redes sociales y de los restantes medios sociales como *blogs, wikis, mashups* (de modo autónomo o integrados en redes sociales). A lo que se une la difusión de tecnologías en torno a la Geolocalización, Realidad Aumentada, la Web en tiempo real o el Internet de las cosas (acceso a la Red mediante todo tipo de "cosas", sensores, electrodomésticos, herramientas tecnológicas, etc.) [15].

¿Qué implica este desarrollo tecnológico desde el punto de vista de la conceptualización de las ciberamenazas? Que no podemos ignorar los abrumadores cambios sociales que esto conlleva, ni que *all disruptive technologies upset traditional power balances […] The standard story is that empower the powerless, but that's only half the story. Empowers everyone. And changed social power*[16].

Ese empoderamiento social no es negativo, muy al contrario, como venimos diciendo es necesario fomentar la confianza y el conocimiento y manejo activo de todas esas tecnologías, pero, como también hemos señalado, ello debe ir acompa-

[14] GALDON CLAVELL, G., "Big Data y miopía de la Administración", *El País*, Acceso: 19 de marzo de 2014.

[15] *Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el Ciberespacio*, Cuadernos de Estrategia, núm. 149, Ministerio de Defensa, 2011.

[16] SCHNEIER, B., "Power and the Internet", *What *should* we be worried about?*, Annual question 2013, http://edge.org/response-detail/23818. Acceso: 31 de marzo de 2014.

ñado de la evolución y adaptación adecuada de nuestra democracia, para que siga siendo tal en este nuevo mundo.

Si no se asume el cambio social, el empoderamiento de diversos sectores ciudadanos y empresariales, y no se toman medidas adecuadas como la adaptación de los entornos legislativos, por ejemplo, o la adopción de políticas corporativas de movilidad, sino que se reacciona, en aras de un concepto de seguridad erróneo, con una continua proliferación de normas de "seguridad y protección" –regulaciones administrativas, normativas internas, etc.- incompatibles con la realidad de ese cambio social, el resultado es una brecha de seguridad constante, que ni las herramientas de seguridad informática más sofisticadas (SEM, *sandboxing* dinámico, *Security Analytics*, etc.) van a conseguir paliar.

El usuario, sea más o menos experto, sea un ciudadano particular en el desarrollo de actividades de ocio, un administrado en sus relaciones con la Administración, un empleado público en su puesto en un Ministerio, o en un servicio público, un trabajador de una empresa privada, etc., es el que tiene en sus manos la última barrera de una línea de defensa profunda en el ámbito de la seguridad nacional. Por tanto, debe ser concienciado en todas sus facetas, debe ser formado y se le debe proporcionar un entorno democrático reconocedor del cambio social operado por las nuevas tecnologías, puesto que *en la ciberdefensa pasiva deben participar todos los ciudadanos, administraciones, instituciones y empresas del Estado, cada uno a su nivel y con sus medios (paradigmas de la guerra total y de la guerra asimétrica)*[17].

Todo lo anteriormente expuesto, no es óbice para, una vez tomada en cuenta la dimensión global del ciberespacio y la necesidad de una defensa global en profundidad con varias barreras entre las que la participación y concienciación de ciudadanos, Administraciones y empresas son imprescindibles, proceda igualmente tener en cuenta que el análisis de dimensiones concretizadas del riesgo global, lo que la Estrategia de Seguridad Nacional identifica como ciberamenazas, sea también necesario, y sea abordado desde un punto de vista que, trascendiendo la dimensión de la seguridad, pase a activar una defensa –e incluso ataque- con rasgos específicamente militares, y donde encontramos, entre otras cuestiones, la dificultad de delimitar los significados, estrategias y/o intenciones presentes tras las acciones, la dificultad de asignar la atribución real de los ataques y una asimetría entre el atacante y el atacado.

3. EL PAPEL DE LA DEFENSA NACIONAL EN LA ESN

El hecho de que las ciberamenazas pueden afectar a la Defensa Nacional no puede considerarse una novedad. Desde hace décadas se viene advirtiendo sobre

[17] Ministerio de Defensa, *Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario*, Monografías, núm. 137, CESEDEN, 2013, p. 15.

la posibilidad de que este fenómeno pueda presentar la efectividad suficiente para constituir un riesgo de tal índole[18]. De tal modo, la ENS, como no podía ser de otra manera, contempla las ciberamenazas como uno de los riesgos y amenazas que pueden afectar, en primer lugar a la Seguridad Nacional para, en un segundo paso, poner de relieve la forma en que esas ciberamenazas pueden constituir, asimismo, un riesgo para la Defensa Nacional.

Así, su Capítulo 3 afirma que la exposición de España a los ciberataques genera, no sólo elevados costes económicos, sino también y lo que es más importante, la pérdida de confianza de los ciudadanos en unos sistemas que, en la actualidad, resultan críticos para el normal funcionamiento de la sociedad.

Las líneas de acción estratégica, desarrolladas en el Capítulo 4 del mismo documento, comienzan por la Defensa Nacional entendiendo que su objetivo principal está constituido por los conflictos armados que se puedan producir como consecuencia, tanto de la defensa de los intereses o valores exclusivamente nacionales –en los que se intervendría de manera individual– como de la defensa de intereses y valores compartidos en virtud de nuestra pertenencia a organizaciones internacionales tales como la ONU, la OTAN o la UE, en los que se intervendrá conforme a sus tratados constitutivos junto con otros aliados o socios sin hacer, pues, alusión expresa a las amenazas o riesgos que pudieran provenir de los ataques informáticos.

Continúa la ENS definiendo sus líneas de acción estratégicas, entre las que se encuentra, en primer lugar y por lo que a la Defensa Nacional se refiere, la provisión de capacidades militares que permitan el cumplimiento de las misiones asignadas, así como un nivel de disuasión creíble. En todo caso, afirma el citado documento, la Defensa Nacional mantendrá las capacidades necesarias para reaccionar y neutralizar cualquier riesgo o amenaza de orden militar.

Aunque a primera vista pudiera parecer que la ESN no relaciona la intervención de la Defensa Nacional respecto de las ciberamenazas, sin embargo, la conjunción de ambos objetivos aquí descritos, conduce a una conclusión distinta. La posibilidad de que ese riesgo o amenaza de orden militar se produzca a través de una ciberamenaza no resulta en modo alguno extraño. Si bien es verdad que el mismo documento focaliza los riesgos que puede sufrir nuestro país a las amenazas cibernéticas que generan, principalmente, costes económicos, los ataques que han sido sufridos por países de nuestro entorno hacen que la posibilidad de que los medios a disposición de la Defensa Nacional tengan que entrar en acción, no resulte improbable. Máxime cuando el mencionado Capítulo 4 recuerda la obligación de hacer frente a los conflictos armados si ello se deriva del cumplimiento de nuestras obligaciones con las Organizaciones Internacionales de las que España es parte.

[18] Así se manifestaban John Arquilla y David Ronfeldt, en su obra "Cyberwar is Coming!", Comparative Strategy, Vol. 12, No. 2, Spring 1993, pp. 141–165.

Esta visión ha resultado ratificada y completada a través de la publicación de la Estrategia de Ciberseguridad Nacional, cuya primera línea de acción consiste en "*Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional*" lo que, según su propio texto, ha de llevarse a cabo adoptando una serie de medidas entre las que se encuentran ampliar y mejorar permanentemente las capacidades de Ciberdefensa de las Fuerzas Armadas que permitan una adecuada protección de sus Redes y Sistemas de Información y Telecomunicaciones, así como de otros sistemas que afecten a la Defensa Nacional. La Estrategia de Ciberseguridad Nacional, asimismo, reconoce la importancia de consolidar la implantación del Mando Conjunto de Ciberdefensa y potenciar su cooperación con los diferentes órganos con capacidad de respuesta ante incidentes cibernéticos en aspectos de común interés. Por último, prevé potenciar las capacidades militares y de inteligencia para ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio, ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

Este Mando Conjunto de Ciberdefensa (MCCD) al que la Estrategia de Ciberseguridad Nacional alude, fue creado por la Orden Ministerial 10/2013[19]. La propia Exposición de Motivos de dicha Orden Ministerial resalta la necesidad contar con la disposición de capacidades adecuadas y la determinación de utilizarlas si fuera necesario. En consecuencia, prevé que el Ministerio de Defensa participe en el impulso de una gestión integral de la ciberseguridad, en el marco de los principios que se establezcan al efecto en la Estrategia de Ciberseguridad Nacional, que ya han sido aquí mencionados.

De esta forma, se implica a las Fuerzas Armadas en la salvaguarda de la ciberseguridad nacional, no limitándose su papel a la protección de los sistemas de utilización puramente militar. Para ello, su ámbito de actuación se desarrollará tanto en las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, como en aquéllas otras que específicamente le sean encomendadas y que afecten a la Defensa Nacional[20].

Aquí estriba uno de los principales retos que se plantean en la implantación de las líneas de acción descritas, que no es otro que discernir en qué momento o bajo qué circunstancias, un ataque cibernético conllevará la actuación de los medios puestos a disposición de la Defensa Nacional. En este sentido es importante

[19] La Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas fue publicada en el Boletín Oficial de Defensa núm. 40, de 26 de febrero de 2013.

[20] Así puede leerse en el artículo 3 de la repetida Orden Ministerial.

hacer notar que el uso de las tecnologías con fines bélicos no reviste una única modalidad. Antes bien, el estudio de supuestos reales pone de relieve que nos encontramos ante un fenómeno que reviste diversas modalidades cuya relevancia difiere enormemente enter sí. Desde la mera actividad o agitación colectiva a través de redes sociales hasta el lanzamiento de un ataque informático que pudiera considerarse un ataque armado, pueden contemplarse una gran variedad de supuestos.

Es aquí donde la labor de los juristas resulta determinante pues esa distinción de supuestos que abarcan desde actuaciones inofensivas a la realización de actos de guerra, en un contexto bélico, requerirá una distinta respuesta desde el punto de vista jurídico. En cualquier caso, parece claro que podemos encontrarnos ante lo que podrían considerarse tres categorías esenciales, determinantes para la calificación jurídica de los hechos, cuyas manifestaciones son la ciberguerra, las ciberoperaciones y los ciberataques[21].

Es dentro de éstos últimos donde la delimitación se hace más difícil, por cuanto no resulta evidente en qué momento un ciberataque sobrepasa la entidad de un delito común o de una mera actividad de protesta para entrar dentro de lo que podría considerarse como un "ataque armado" y, por tanto, dar lugar a una respuesta en la que hubiera de entrar en juego la Defensa Nacional. En relación al primero de los supuestos, la regulación jurídica puede considerarse relativamente satisfactoria. En nuestro ámbito interno la mayoría de las actividades delictivas cometidas por la red han encontrado su correspondiente respuesta penal[22] y, desde el punto de vista del Derecho Internacional, no puede olvidarse la regulación del Convenio del Consejo de Europa sobre Ciberdelincuencia de 2001. En este sentido es claro, siguiendo a GONZALEZ CUSSAC que cibercrimen y ciberamenazas no son categorías equivalentes, por cuanto la comisión de un delito informático o de un delito, que puede que podríamos llamar "convencional" a través de medios cibernéticos, no tiene porqué constituir una amenaza a la seguridad nacional ni, evidentemente, todas las amenazas a la seguridad nacional provienen de los delitos mencionados. Sin embargo, como afirma este autor, es evidente que determinados ciberdelitos o delitos cometidos

[21] Así se expresan DE TOMÁS MORALES, S. y VELÁZQUEZ ORTIZ, A.P. en el trabajo de investigación "La responsabilidad del Mando en la conducción de las operaciones durante la ciberguerra: la necesidad de un adiestramiento eficaz", galardonado con el Premio Defensa 2013, en la modalidad "José Francisco de Querol y Lombardero", que puede consultarse en el enlace: www. portalcultura. mde.es/actividades/ premios/ defensa/2013/. Dicho trabajo de investigación se encuentra pendiente de ser publicado en la *Revista de Derecho Militar* (núm. 100).

[22] De este modo se recogen en el Código Penal español, tanto los llamados delitos informáticos, como los delitos hasta ahora conocidos que pueden ser cometidos por medios virtuales. Véase respecto de los primeros la regulación de los artículos 256, 264 y 265, así como los artículos 183 bis), relativo los delitos contra la libertad sexual o a título de ejemplo, los artículos 270 a 280, en relación a los delitos contra la Propiedad intelectual e industrial.

por internet, sí pueden representan una amenazas a la seguridad nacional[23]. Si el deslinde, pues, entre las actividades criminales cometidas contra o a través de internet y el riesgo para la Seguridad Nacional, no siempre se revela evidente, más difícil resulta determinar en qué momento esa actividad supone un riesgo o amenaza efectiva para la Defensa Nacional. Es decir en qué momento esa actividad, en principio con apariencia delictiva, reúne los elementos necesarios para ser considerada un ataque.

La OM ya citada, poco desvela en este punto, pues en su artículo 4, dedicado a explicitar la misión atribuida al MCCD, únicamente atiende al "*planeamiento y la ejecución de las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional*", sin que al respecto se ofrezca ninguna definición sobre cuáles sean éstos.

Por tanto, el reto que tanto la ESN al hablar de las ciberamenazas, como la Estrategia de Ciberseguridad y aun la Orden 10/2013 de creación del MCCD plantean, resulta eminentemente jurídico, en tanto que de la definición que, desde este ámbito, se dé respecto del ciberataque dependerá la intervención o no de la Defensa Nacional a través de este Mando Conjunto, siendo posible así, articular la respuesta que el artículo 5 de la Orden 10/2013 prevé para estos casos.[24]

A pesar de que los esfuerzos de la Comunidad Internacional por la consecución de una regulación jurídica de internet se remontan a los años 90[25], es evidente que semejante tarea no ha sido consumada. Sigue pendiente, por tanto, no sólo una regulación de este nuevo ámbito sino también una concreción de determinados conceptos jurídicos que, inevitablemente, han de ser ahora interpretados al objeto de incluir el elemento virtual, de modo que queda por preguntarse cuándo nos encontramos ante un ataque armado proveniente de internet, conforme al Derecho Internacional Convencional y Consuetudinario.

---

[23] En este sentido, puede consultarse GONZÁLEZ CUSSAC, J. L., "Estrategias legales frente a las ciberamenazas". Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, en Cuadernos de Estrategia. Número 149. Instituto Español de Estudios Estratégicos. Instituto Universitario «General Gutiérrez Mellado». Diciembre 2010.Pág. 92.

[24] El artículo 5 de la Orden 10/2013, señala que, entre los cometidos del MCCD se encuentra ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

[25] Así se pone de manifiesto por SÁNCHEZ DE ROJAS DÍAZ, E., "Cooperación Internacional en temas de seguridad, en Necesidad de una conciencia nacional…., pág 273. Doc. cit, en cita 17 *supra*, cuando afirma que la cuestión de la seguridad de la información ha estado en la agenda de la ONU desde que la Federación de Rusia en 1998 introdujo por primera vez un proyecto de resolución en la Primera Comisión de la Asamblea General de la ONU.

4. LOS CIBERATAQUES COMO AMENAZA A LA DEFENSA NACIONAL. ASIMILACIÓN DE LOS CIBERATAQUES AL CONCEPTO DE ATAQUE ARMADO

Han sido muchos los documentos emanados por las Organizaciones Internacionales que han puesto de relieve la necesidad de contemplar el elemento cibernético como objetivo militar y como un método de combate, idóneo para realizar ataques de dicha naturaleza[26].

De esta forma, si la Defensa Nacional entra en juego en aquéllos supuestos en que un Estado es víctima de un ataque armado, será preciso analizar en qué situaciones un ciberataque constituye un ataque armado equiparable al que podría darse con la utilización de medios y métodos de combate que podríamos llamar convencionales.

En este sentido, resulta evidente que la interpretación analógica conlleva una serie de riesgos desde el punto de vista de la seguridad jurídica[27], pero no es menos cierto que constituye una institución jurídica consolidada como método interpretativo que, incluso, se impone en determinados casos como es el presente.

En consecuencia, habrá que comenzar por dirimir si ese ataque informático puede considerarse o no, incluido en la prohibición del "uso de la fuerza" y la amenaza a través del mismo, que establece el artículo 2 de la Carta de Naciones Unidas[28]. Sólo así será posible distinguir aquéllos ataques informáticos que podemos entender constitutivos de un delito cibernético o de una actividad incluso inofensiva, de aquéllos otros que podrían originar una respuesta armada.

El artículo 2, de la Carta de Naciones Unidas en su apartado 4 expresamente establece:

> "*Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas*".

[26] En este sentido se expresó el documento resultante de la XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja que se celebró en Ginebra, entre noviembre y diciembre de 2011, cuyos resultados pueden ser consultados en el siguiente sitio web: http://www.icrc.org/spa/index.jsp. Dicho documento puso de relieve el hecho de que cualquier medio, conectado a Internet, puede convertirse en un objetivo que puede ser atacado, desde cualquier parte del planeta. Por otra parte, la OTAN, en su Documento "Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation", adoptado en Lisboa, en 2010, afirma: "Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks". Puede ser consultado en http://www.nato.int/cps/en/natolive/official_texts_68580.htm.

[27] RABOIN, B., en "Corresponding Evolution: International…", doc. cit., en cita 28 *supra*. p. 624.

[28] Carta de Naciones Unidas firmada en San Francisco, Estados Unidos, el 26 de junio 1945.

Muchas han sido las interpretaciones que a este artículo se han dado por parte de la doctrina, por cuanto el propio concepto de *uso de la fuerza* no ha resultado pacífico, incluso con anterioridad a la aparición de este elemento cibernético. La Resolución 2625 de Naciones Unidas proclama, entre otros el principio de que los Estados, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los propósitos de las Naciones Unidas.[29] Por otra parte, la Resolución 3314 de 1974[30] de la misma Organización, define la agresión como "*el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado o en cualquier otra forma incompatible con la Carta de las Naciones Unidas, tal como se enuncia en la presente Definición*". Sin embargo, no parece que dicha definición aporte demasiada claridad al problema planteado, por cuanto, el principal interrogante sigue sin esclarecerse. Es decir, hasta qué punto la utilización de un ataque informático puede considerarse equivalente al ejercicio de la fuerza armada o lo que es lo mismo, en qué medida podemos considerar que internet es un arma asimilable a cualquier otra de carácter convencional. Tampoco la enumeración realizada por la citada Resolución de los actos que, con independencia de la existencia de una declaración de guerra, han de considerarse un acto de agresión, aporta, a los efectos que aquí conciernen, una solución incontrovertible[31].

---

[29] Resolución 2625 (1970), adoptada por la Asamblea General en su 25ª, de 24 de octubre 1970. Contiene la declaración relativa a los principios de Derecho Internacional referentes a las relaciones de amistad y a la cooperación entre los estados de conformidad con la carta de las naciones unidas. Doc. A/RES/25/2625.

[30] Resolución 3314 (1974), adoptada por la Asamblea General en su 2319ª sesión plenaria, de 14 de diciembre de 1974. Doc. RES/3314 (1974).

[31] La Resolución mencionada entiende que son actos de agresión los enumerados en su artículo 3, que reza como sigue:

a) La invasión o el ataque por las fuerzas armadas de un Estado del territorio de otro Estado, o toda ocupación militar, aun temporal que resulte de dicha invasión o ataque, o toda anexión, mediante el uso de la fuerza, del territorio de otro Estado o de parte de él.

b) El bombardeo, por las fuerzas armadas de un Estado del territorio de otro Estado, o el empleo de cualesquiera armas por un Estado contra el territorio de otro Estado.

c) El bloqueo de los puertos o de las costas de un Estado por las fuerzas armadas de otro Estado.

d) El ataque por las fuerzas armadas de un Estado contra las fuerzas armadas terrestres navales o aéreas de otro Estado, o contra su flota mercante o aérea.

e) La utilización de fuerzas armadas de un Estado, que se encuentran en el territorio de otro Estado con el acuerdo del Estado receptor, en violación de las condiciones establecidas en el acuerdo o toda prolongación de su presencia en dicho territorio después de terminado el acuerdo.

f) La acción de un Estado que permite que su territorio, que ha puesto a disposición de otro Estado, sea utilizado por ese otro Estado para perpetrar un acto de agresión contra un tercer Estado.

g) El envío por un Estado o en su nombre de bandas armadas, grupos irregulares o mercenarios que lleven a cabo actos de fuerza armada contra otro Estado de tal gravedad que sean equiparables a los actos antes enumerados, o su sustancial participación de cipos actos.

En cualquier caso, hay que tener siempre presente que la prohibición del uso de la fuerza constituye una norma de aplicación universal toda vez que se trata de Derecho consuetudinario, aplicable, por tanto a cualquier Estado, tal y como establece la Sentencia de la Corte Internacional de Justicia en relación a las actividades militares y paramilitares en y contra Nicaragua, de 27 de junio de 1986[32].

Dentro de los tradicionales métodos interpretativos para determinar si un ataque cae dentro de la definición de agresión ofrecida por Naciones Unidas, cobra fuerza la teoría interpretativa basada en los resultados[33]. Abandonando así el tradicional método de determinar la existencia del uso de la fuerza, basado en la naturaleza del ataque, se expone la teoría que aboga por considerar los efectos que pueda tener un ataque cibernético para, de este modo, determinar la adecuación del mismo al Derecho Internacional. En efecto, cabe precisar que la teoría basada en la naturaleza del ataque no puede resultar completamente adecuada en este caso, por el hecho de que nos encontramos con un tipo de amenazas que no responden de forma idéntica a la naturaleza de las que hasta ahora resultaban conocidas. Ello, incluso, ha dado lugar a un cambio en la propia concepción de los conflictos que incluyen el elemento cibernético como una parte esencial en el desarrollo de los conflictos convencionales.[34]

Es evidente que algunos ciberataques podrían causar un daño efectivo, real y equiparable al que podría suponer el empleo de la fuerza cinética[35]. Así, puede afirmarse que la naturaleza de los ataques informáticos que hasta ahora han provocado mayor alarma en la Comunidad Internacional, revisten dudas en cuanto a su catalogación como ataques armados o uso de la fuerza[36]. Además, teniendo en consideración el contexto en el que algunos de ellos se han producido, podrían haber originado una respuesta por parte del Estado víctima de los mismos que,

---

[32] Así queda establecido en el Parágrafo 209 de la Sentencia relativa a Military and Paramilitary Activities in and Against Nicaragua (*Nicar. v. U.S.*), 1986 I.C.J. 14.

[33] Así se expresa Raboin, B. en el artículo "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", *Cleveland State Law Review*, (núm.31, 2013), pp. 603-668, que puede ser consultado a través del enlace: http://digitalcommons.pepperdine.edu/naalj/vol31/iss2/5. Acceso: 31 de marzo de 2014.

[34] En este sentido se expresó, en julio de 2011, el Departamento de Defensa de los Estados Unidos, al publicar la Estrategia para las Operaciones en el Ciberespacio, documento que parte de la base de que la Seguridad Nacional ha de ser redefinida a través del concepto de ciberespacio y que, tanto, las operaciones militares, como las de Inteligencia y las comerciales dependen del ciberespacio para ser realizadas con éxito; *Strategy for Operating in Cyberspace, Department of the Army*, 2011 en: www.ieee.es/ Galerias/ fichero/OtrasPublicaciones/Internacional/ ResenaEstrategiaoperacionesCiberespacio_julio2011.pdf.

[35] RABOIN, B., en "Corresponding Evolution: International,…, *op. cit.*, en cita 33 *supra*.

[36] Estos recientes y más considerables ataques han sido objeto de estudio fundamentalmente por parte de la OTAN, principalmente a través de su Centro de Excelencia de Ciberdefensa entre cuyas múltiples publicaciones, en este sentido, puede destacarse la siguiente: Tikk, E., *International Cyberincidents. Legal considerations*, CCDCOE, 2010. Disponible también en formato digital, a través de la web: www.ccdcoe.org. Acceso: 29 de marzo de 2014.

igualmente, hubiera supuesto una contravención al Derecho Internacional. Tal es el caso más reciente de los ataques recibidos por Ucrania durante el conflicto interno sufrido a lo largo del último invierno, así como en el desarrollo de las tensiones diplomáticas con Rusia[37]. En semejante contexto, la recepción de un ataque informático por parte de Ucrania, podría haber sido interpretado como un acto de agresión.

Atendiendo, una vez más a las Resoluciones de Naciones Unidas, resulta obligado recordar que la Resolución 3314, anteriormente citada, establece, taxativamente, que la enumeración de actos de agresión recogida en el precedente artículo 3 no resulta de carácter exhaustivo. Antes bien, dicha enumeración queda supeditada a que el Consejo de Seguridad de Naciones Unidas, determine, en un momento dado, qué otros actos constituyen agresión con arreglo a las disposiciones de la Carta.

Pues bien, en el referido supuesto de los ataques cibernéticos sufridos por Ucrania no se ha producido dicho pronunciamiento, como tampoco en relación a otros que ya habían sido constatados con anterioridad en el tiempo, en similar contexto[38]. No obstante, en atención a los criterios interpretativos expuestos y teniendo en cuenta los efectos de los que se tiene conocimiento, sufridos por Ucrania, no parece que los mismos constituyan un ataque de la envergadura suficiente para tener la consideración de "uso de la fuerza" o "ataque armado".

El concepto de uso de la fuerza ha sido también estudiado desde una perspectiva que implica el análisis de los conceptos de violencia armada, fuerza coercitiva o fuerza de interferencia[39]. Desde este punto de vista, se entiende que sólo la fuerza física armada queda prohibida por el artículo 2 (4) de la Carta de Naciones Unidas y que la definición de ataque armado es mucho más restrictiva que la de uso de la fuerza utilizada por la Carta de Naciones Unidas, de forma que puede haber actos que violen la prohibición del artículo 2(4) y que, sin embargo, no constituyan un ataque armado, que, tal como hace constar De LUCCA, puede

---

[37] De todos estos hechos ha dado cuenta la prensa internacional, pudiendo consultarse en este sentido la página web www.bbc.com, cuya publicación *on line* de 5 de marzo de 2014, refería los ataques producidos afirmando: LEE, D.E "Security forces in Ukraine have accused the Russian army of disrupting mobile communications. Smaller-scale attacks have seen news websites and social media defaced with propaganda messages". http://www.bbc.com/news/technology-26447200.

[38] De entre todos los ciberataques de los que a diario se tiene conocimiento, han sido los sufridos por Georgia en el año 2008, los que han sido objeto de una atención especializada, de nuevo por parte de OTAN, hasta el punto de la publicación monográfica por el ya mencionado Centro de Excelencia de la obra: TIKK, E. y otros, *Cyber Attacks Against Georgia: Legal Lessons Identified*, CCDCOE, 2008. Igualmente disponible en formato digital a través de la página web oficial del Centro de Excelencia www.ccdcoe.org.

[39] DE LUCCA, C.D., "The Need for International Laws of War to Include Cyber Attacks Involving State and Non- State Actors", *Pace International Law Review Online Companion. School of Law* (Vol. 3:9, enero 2013), p. 294.

encontrarse en la mencionada Sentencia de la Corte Internacional de Justicia[40]. Siguiendo la presente construcción teórica que impone un criterio interpretativo como el expuesto, cabe plantearse las consecuencias prácticas de su aplicación. Así, si el artículo 2 (4) de la Carta prohíbe exclusivamente el uso de la fuerza física, el lanzamiento del virus Stuxnet[41] no resultaría recogido dentro de la prohibición. Es decir, la introducción del virus Stuxnet no podría ser considerada la realización de un acto de fuerza por cuanto las centrales nucleares de Irán, en ningún momento, fueron atacadas por la fuerza física y tampoco puede concluirse que fuera un ataque armado, según la definición dada más arriba en tanto que no parece la forma más grave de uso de la fuerza.

El reciente y controvertido lanzamiento de este virus también puede servir de ejemplo para revelar la dificultad de la conceptuación no sólo de este supuesto sino de los ataques informáticos, en general. Añadiendo a esta labor un criterio adicional, podría examinarse el repetido virus Stuxnet a la luz de la teoría que aúna los criterios relativos a la instrumentalidad del ataque, el objetivo de dicho ataque y las consecuencias del mismo[42]. De esta forma, en función del criterio de la instrumentalidad, un ciberataque no constituye un ataque armado de acuerdo con el artículo 2(4) toda vez que carece de las características físicas que, tradicionalmente, han sido asociadas a los ataques militares. Para HOLLIS, la Carta de las Naciones Unidas ofrece cierto apoyo a esta visión por cuanto su artículo 41 al enunciar las medidas que no involucran el uso de fuerza armada, incluye las "*interrupciones completas o parciales de telegrafía, radio, y otros medios de comunicación*". Sin embargo, aun abogando por una interpretación basada en criterios restrictivos, no puede contemplarse la anterior teoría como una fórmula adecuada a la naturaleza y gravedad de las situaciones a las que, con toda seguridad, la Comunidad Internacional deberá hacer frente en un futuro. Excluir los ataques informáticos del concepto de ataque armado por el hecho de no compartir las características físicas de los ataques militares, conocidos hasta ahora y por la exclusión conceptual realizada por el artículo 41 de la Carta, conllevaría un agravamiento de la situación jurídica actual. Por otra parte, la interpretación expuesta en relación al contenido del artículo 41, tampoco resulta viable en este ámbito por cuanto, en la actualidad internet no puede ser considerado, exclusivamente, como un medio

---

[40] De Lucca, C.D., "The Need for International Laws", *op. cit.*, en cita 39, p. 295.

[41] El virus Stuxnet ha sido definido por algunos autores como: "….start of a new era in the arms-race in cyber security. First time in history, a targeted cyber attack was discovered that aimed at physically destroying part of the critical infrastructure of a state". Así se expresan Bencsath B., y otros, en el artículo "The Cousins of Stuxnet: Duqu, Flame, and Gauss", *Future Internet* (núm. 4, 2012) pp. 971-1003; doi:10.3390/fi4040971. Disponible en www.mdpi.com/journal/futureinternet. Acceso 25 de marzo de 2014.

[42] HOLLIS, D.B., "Why States Need an International Law for Information Operations", *11 LEWIS & CLARK L. REV.* (núm. 1023, 1093, 2007), pp. 1023-1061.

de comunicación, una vez que ha quedado sobradamente demostrado que sus capacidades son infinitamente mayores.

Si dentro de esta conjunción de criterios analizamos el objetivo del ataque, resulta que un ciberataque constituirá uso de la fuerza siempre y cuando penetre en las infraestructuras críticas, incluso aun cuando no cause daños físicos. Esta construcción teórica presenta el problema de ser excesivamente amplia, por cuanto los efectos de un ciberataque pueden abarcar, como se ha expresado anteriormente, un gran rango de actividades: desde mera propaganda a actividades potencialmente peligrosas e incluso destructivas. En efecto, en aplicación de este criterio un ciberataque dirigido a infraestructuras críticas, como lo fue el caso de Stuxnet, podría resultar incluido dentro del concepto de uso de la fuerza, pero también lo estarían aquéllos que resultaran netamente inoperantes o inofensivos.

Si, por otro lado, se atiende al criterio que propone tomar en consideración las ocasionales consecuencias de un ataque cibernético, puede concluirse que un cibertaque constituirá uso de la fuerza siempre que su pretensión sea causar los mismos efectos que podría generar un ataque producido por fuerza cinética. En el repetido caso de la introducción del virus Stuxnet en la central nuclear iraní, no cabe duda de que sus efectos, *a priori*, se concretaron en la neutralización del desarrollo del enriquecimiento de uranio por el Estado aludido[43]; resultado éste que, en efecto, podría asimilarse al obtenido en el uso de otro tipo de armas.

Aun de forma breve, no puede dejar de mencionarse que la construcción teórica relativa a la prohibición del uso de la fuerza, necesariamente, ha de complementarse con el Derecho consuetudinario que establece la prohibición de los Estados de intervenir en los asuntos internos de otros Estados. Así quedó establecido por la sentencia de la Corte Penal Internacional en el caso de las actividades militares en y contra Nicaragua que determinó que, en los supuestos en que la injerencia tomara forma de uso o amenaza de la fuerza, el Derecho consuetudinario de no intervención resulta colindante con el artículo 2 (4) de la Carta de Naciones Unidas[44].

Es innegable, por último, que el uso de la fuerza utilizado en respuesta a un ciberataque deberá cumplir con los principios de necesidad y proporcionalidad establecidos, asimismo, por el Derecho consuetudinario[45].

---

[43] BROAD, W.J., y otros, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, 15 January 2011. Asimismo la cadena británica BBC informa sobre lo sucedido, en fecha 15 de febrero de 2011. FILDES, F., *Stuxnet Virus Targets and Spread Revealed*. http://www.bbc.co.uk/news/technology- 12465688.

[44] Military and Paramilitary Activities in and Against Nicaragua (*Nicar. v. U.S.*), 1986 I.C.J. 14, para. 209 (June 27): *The Court therefore finds that no such general right of intervention, in support of an opposition within another State, exists in contemporary international law. The Court concludes that acts constituting a breach of the customary principle of non-intervention will also, if they directly or indirectly involve the use of force, constitute a breach of the principle of non-use of force in international relations*.

[45] Así se expresan HATHAWAY, O. A., y otros, en "The law of cyber-attack", *Yale Faculty Scholarship Series*, (paper 3852, 2012), pp. 817-886.

En consonancia con lo expuesto hasta ahora y, habida cuenta la previsión contenida en el Capítulo 4 de la ENS, dedicado a las líneas de acción estratégica, que recuerda la obligación de hacer frente a los conflictos armados que se puedan producir como consecuencia de la defensa de intereses y valores compartidos en virtud de nuestra pertenencia a organizaciones internacionales y teniendo en cuenta la pertenencia de España a la OTAN, resulta preciso hacer una específica mención al artículo 5 del Tratado del Atlántico Norte. El mismo establece que un ataque armado contra una o más de las Partes del mismo que tenga lugar en Europa o en América del Norte será considerado como un ataque dirigido contra todas ellas y, en consecuencia, si tal ataque se produce cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva, reconocido por el artículo 51 de la Carta de las Naciones Unidas, se comprometen a ayudar a la Parte o Partes atacadas, adoptando, seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte. Cualquier ataque armado de esta naturaleza y todas las medidas adoptadas en consecuencia serán, inmediatamente, puestas en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las disposiciones necesarias para restablecer y mantener la paz y la seguridad internacionales.

Nuevamente, resulta determinante examinar el concepto de "ataque", a la vista de los nuevos métodos que pueden ser empleados en su desarrollo. A la luz de los criterios hasta ahora expuestos no parece imposible atribuir a un ciberataque la calificación jurídica equivalente al ataque que se realice por otros medios, contra un Estado miembro de OTAN. En el examen del Tratado de Washington resulta obligado hacer referencia a la definición que realiza el artículo 6 del Tratado que, expresamente, considera ataque armado contra una o varias de las Partes, el que se produzca contra el territorio de cualquiera de las Partes en Europa o en América del Norte, contra los departamentos franceses de Argelia, contra el territorio de Turquía o contra las islas bajo la jurisdicción de cualquiera de las Partes en la zona del Atlántico Norte al norte del Trópico de Cáncer, así como el que se produzca contra las fuerzas, buques o aeronaves de cualquiera de las Partes que se hallen en estos territorios, o en cualquier otra región de Europa en la que estuvieran estacionadas fuerzas de ocupación de alguna de las Partes, en la fecha de entrada en vigor del Tratado, o que se encuentren en el Mar Mediterráneo o en la región del Atlántico Norte al norte del Trópico de Cáncer.

Nuevamente, el Tratado obvia cualquier definición de ataque armado y circunscribe su aplicación a que éste se produzca en un determinado ámbito territorial. Toda vez que el único criterio que el Tratado de Washington ofrece para determinar si nos encontramos ante un ataque armado es el elemento territorial, resultaría apropiado considerar que los efectos de un ciberataque, siempre se darán en las instalaciones, medios, personas o efectos pertenecientes a un Estado en concreto. Sin embargo,

también parece conveniente poner de relieve que, una vez superada la delimitación que considera posible el desarrollo del conflicto bélico en el espacio terrestre, marítimo y aéreo, se hizo necesario incluir el espacio supraterrestre, de la misma manera que, en este momento, debería tenerse en cuenta la posibilidad de que los conflictos sean librados en un ámbito virtual y no físico[46].

En este punto, resulta necesario hacer notar que la OTAN ha sido, sin duda, una de las Organizaciones que mayor actividad ha desarrollado en la investigación científica en la materia que ahora nos ocupa; hecho éste que no puede resultar extraño, habida cuenta la naturaleza de la propia Organización, así como el número de ataques sufridos por alguno de sus Estados miembros y aun por su propia página web[47].

En el desarrollo de esta actividad, la OTAN ha patrocinado la publicación del llamado Manual de Tallín[48] en el que, entre otras cuestiones, se dirime la posibilidad de asimilar jurídicamente los ciberataques a los ataques armados cometidos a través del uso del armamento convencional. En el ámbito que aquí se analiza, los autores de la obra consideran que una ciberoperación constituirá uso de la fuerza cuando ello resulte de la combinación de, al menos, siete factores que son enumerados y someramente explicados en la Regla 11 del citado Manual. Dichos factores que están constituidos por la severidad del ataque, su inmediación, el efecto directo causado, la invasividad, la posibilidad de medir sus efectos, el carácter militar de dicho ataque y la posible implicación en el mismo, de un Estado. Se propone por parte de los autores un análisis de los ataques cibernéticos basado en la conjunción de estos criterios que, a su juicio, permitirá determinar si el mismo constituye o no, un ataque armado[49]. Así, esa aplicación conjunta de los referidos criterios, parece abogar por una perspectiva restrictiva que, sin duda, permitirá descartar de la inclusión en el concepto de uso de fuerza aquéllos ciber-

---

[46] En este sentido, puede consultarse GÓMEZ DE AGREDA, A., "El ciberespacio como escenario del conflicto. Identificación de las amenazas. El Ciberespacio nuevo escenario de confrontación", *Monografías CESEDEN*, (núm. 126, Febrero 2012), pp. 169-203.

[47] Estos ataques fueron constatados una vez la OTAN se manifestó contraria a la actividad de Rusia en relación a Ucrania. La web oficial de la OTAN incluyó un vídeo en el que expresaba su postura en dicho conflicto. De tales ataques informó la prensa internacional, en fecha 16 de marzo de 2014, tal como puede consultarse http://es.reuters.com/article/topNews/idESMAEA2F00620140316.

[48] Así se conoce comúnmente a la obra conjunta, *Manual on the International Law Applicable to Cyber Warfare*., Cambridge University Press, 2013. Esta publicación recoge la opinión de académicos de referencia en la materia, ofreciendo, así, una opinión colectiva en determinados aspectos controvertidos.

[49] Estos mismos criterios habían sido ya propuestos por SCHMITT, M., en "Cyber operations and the *jus ad bellum* revisited", publicado en *Villanova Law* Review, (Vol. 56. Diciembre 2011), pp. 569- 606 y recogidos en FOLTZ, A.C., en "Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate", *JFQ* (issue 67, 4th quarter 2012), pp. 40-48. Disponible en formato digital en www.ndupress.ndu.edu, así como en ZIOLKOWSKI K., "Ius ad bellum in "Cyberspace – Some Thoughts on the "Schmitt- Criteria" for Use of Force", en el libro CZOSSECK, C. y otros, *2012 4th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, 2012. Disponible en la página web del Centro de Excelencia: www.ccdcoe.org.

taques de menor entidad. Desde este punto de vista y, aun teniendo en cuenta las prevenciones realizadas por los autores de la obra relativas a la necesidad de contextualizar los ciberataque, no parece generar dudas que la categorización del virus Stuxnet como una materialización del uso de la fuerza. No puede concluirse de la misma forma, sin embargo, respecto a los ataques sufridos por la OTAN en su página web que, difícilmente, podrían verse encuadrados en algunos de los criterios expuestos tales como la severidad de los mismos o su carácter militar.

Esta tesis restrictiva parece responder de forma más fiel a la normativa internacional que ha sido examinada y, a pesar de su complejidad, su aplicación resulta más deseable que la de los criterios expuestos a lo largo del presente estudio. En consecuencia, en tanto no se cuente con una definición de uso de la fuerza que comprenda taxativamente los supuestos en que los ciberataques han de ser incluidos, convendría atender a la citada tesis a la hora de determinar los recursos y medios a disposición de la Defensa Nacional, que la ESN entiende que han de activarse para hacer frente a los conflictos armados, que se puedan producir como consecuencia de la defensa de los intereses o valores nacionales y de los compartidos en virtud de nuestra pertenencia a la ONU, la OTAN y la UE.

5. CONCLUSIONES

La Estrategia de Seguridad Nacional de 2013 ha supuesto un nuevo paso, de gran relevancia, en la construcción y desarrollo de un sistema integrado y convergente de seguridad en nuestro país. Dicha Estrategia se ha visto además complementada por la Estrategia de Ciberseguridad Nacional, también de 2013, que concretiza el sistema diseñado en el ESN en lo que a los aspectos vinculados al ciberespacio y las nuevas tecnologías se refiere.

En una aproximación teórica inicial a estas cuestiones, el presente trabajo ha partido de una reflexión sobre la importancia de la dimensión global de la ciberseguridad en el ámbito del sistema de la seguridad nacional, concluyendo que, si bien la ESN no realiza una plena asunción de dicho carácter eminentemente expansivo de las facetas cibernéticas en la totalidad del sistema de seguridad y defensa del Estado, sí que muestra una clara visión integradora que, en conjunción con la Estrategia de Ciberseguridad Nacional y la Agenda Digital para España, caminan hacia el impulso de la concienciación y formación ciudadana, administrativa y empresarial, con el objetivo de conseguir una adecuada defensa *en profundidad*. A pesar de ello, se concluye también que existen algunas dificultades y lagunas que deberán ser adecuadamente abordados en el marco de los Objetivos establecidos en ambas Estrategias, como es la adecuada adaptación de nuestro sistema democrático a los retos de las nuevas tecnologías, incluido el empoderamiento social, con el fin de reducir los riesgos globales y el impacto

de las ciberamenazas, entendidas como un concepto amplio y expansivo, en la seguridad nacional.

Tras esta conclusión, el presente trabajo se adentra en el análisis de la dimensión específica de la ciberseguridad y en su concreta vinculación con la defensa nacional, profundizando en el hecho de que, aunque a primera vista pudiera parecer que la ESN no relaciona la intervención de la Defensa Nacional con las ciberamenazas (según el concepto delimitado utilizado en la propia ESN), sin embargo, la conjunción de ambos objetivos, conduce a una conclusión distinta. El examen conjunto de ambos aspectos pone de relieve la posibilidad de que un riesgo o amenaza de orden militar se produzca a través de una ciberamenaza, visión que, además, ha resultado ratificada y completada a través de la Estrategia de Ciberseguridad Nacional. La amenaza virtual, por tanto, puede convertirse en riesgo real de modo que sea precisa la actuación de los medios puestos a disposición de la Defensa Nacional.

Sin embargo, puesto que con carácter previo a esa intervención, será preciso examinar en qué supuestos puede equipararse un ciberataque a un ataque armado, hay que tener en cuenta la doctrina contemporánea que ha emprendido dicha labor analítica. Vistos los criterios aportados por la doctrina internacionalista, se hace preciso abogar por aquéllos que, sin abandonar las fuentes del Derecho Internacional, proponen una interpretación restrictiva. Si ante la recepción de un ciberataque, se adoptara una visión excesivamente amplia, ello podría originar la consideración de ataque armado de actividades en la red que, posteriormente podrían revelarse inofensivas o, a lo sumo, meramente delictivas, sin alcanzar la entidad que se exige respecto de un ataque armado. Ello, dada la frecuencia con que se producen estos cibertaques, así como la aparición de los mismos en contextos en los que la tensión política es evidente, podría originar respuestas desproporcionadas y dar lugar, por ende, a un agravamiento de la situación. Se impone por tanto, la adopción de un criterio restrictivo que, en todo caso, proporcione una respuesta a supuestos concretos que ya se han producido, en orden a dar una solución a aquellos otros que en el futuro pudieran producirse en un contexto similar. El criterio definido por los autores del Manual de Tallin, una vez es aplicado no en un plano meramente teórico, sino teniendo en cuenta supuestos concretos de los que se tiene constancia, permite la conceptualización de ciertos ciberataques, como Stuxnet, como ataque armado, con las consecuencias que, desde el punto de vista jurídico, ello podría conllevar.

BIBLIOGRAFIA

ARQUILLA, J. RONFELDT, D., "Cyberwar is Coming!", *Comparative Strategy* (Vol. 12, No. 2, Spring 1993), pp. 141–165.

BENCSATH B., PEK G., BUTTYAN L. y FELEGYHAZI M., "The Cousins of Stuxnet: Duqu, Flame, and Gauss", *Future Internet 2012* (núm. 4, 971-1003; doi:10.3390/fi4040971), en: http:// www.mdpi.com/journal/future-internet.

DE LUCCA, C.D., "The Need for International Laws of War to Include Cyber Attacks Involving State and Non- State Actors", *Pace International Law Review Online Companion. School of Law* (Vol. 3:9, enero 2013), pp. 278 a 315.

DE TOMÁS MORALES, S. y VELÁZQUEZ ORTIZ, A.P. "La responsabilidad del Mando en la conducción de las operaciones durante la ciberguerra: la necesidad de un adiestramiento eficaz". *Premio Defensa 2013, categoría "José Francisco de Querol y Lombardero"*, en: http:// www. portalcultura. mde.es/actividades/ premios/ defensa/2013/.

FOLTZ A.C., "Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate", *JFQ* (issue 67, 4th quarter 2012), pp .40 a 48.

GONZÁLEZ CUSSAC, J. L. "Estrategias legales frente a las ciberamenazas". *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, en Cuadernos de Estrategia* (Núm. 149, Diciembre 2010). pp. 92-102.

GOMEZ DE AGREDA, A., "El ciberespacio como escenario del conflicto. Identificación de las amenazas. El Ciberespacio nuevo escenario de confrontación", *Monografías CESEDEN* (núm. 126, febrero 2012), pp. 169 a 203.

HATHAWAY O. A., CROOTOF R., LEVITZ P., NIX H., NOWLAN A., PERDUE W., SPIEGEL J., "The law of cyber-attack", *Yale Faculty Scholarship Series* (paper 3852, 2012), pp. 817 a 886.

HOLLIS, D. B., "Why States Need an International Law for Information Operations", *11 LEWIS & CLARK L. REV* (1023, 1093. 2007), pp. 1023 a 1061.

MINISTERIO DE DEFENSA, "Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el Ciberespacio", Cuadernos de Estrategia, núm. 149, Ministerio de Defensa, 2011.

MINISTERIO DE DEFENSA, "Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario", *Monografías*, núm. 137, CESEDEN, 2013.

RABOIN, B. "Corresponding Evolution: International Law and the Emergence of Cyber *Warfare", Cleveland State Law Review,* (núm. 31, 2013), pp. 603-668.

SCHMITT M.N., "Cyber operations and the *jus ad bellum* revisited", *Villanova Law Review* (Vol. 56, diciembre 2011), pp. 569-606.

SCHMITT, M. y otros, *Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press 2013.

TIKK E. y otros, *Cyber Attacks Against Georgia: Legal Lessons Identified*, CCDCOE, 2008.
TIKK, E., *International Cyberincidents. Legal considerations*, CCDCOE, 2010.
ZIOLKOWSKI K., "Ius ad bellum in Cyberspace –Some Thoughts on the "Schmitt– Criteria" for Use of Force", en CZOSSECK, C., *2012 4th International Conference on Cyber Conflict.*, NATO CCD COE Publications, Tallinn, 2012.

Otra Documentación (nacional e internacional).

– *Código Penal español*. 20 10/1995 de 23 de noviembre.
– *Convenio Europeo sobre Ciberdelincuencia*. 23 de noviembre de 2001.
– Resolución 2625 (1970) adoptada por la Asamblea General en su 25ª, de 24 de octubre 1970.
– Resolución 3314 (1974), adoptada por la Asamblea General en su 2319ª sesión plenaria, de 14 de diciembre de 1974.
– Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. Boletín Oficial de Defensa número 40 de 2013, 26 de febrero.
– Military and Paramilitary Activities in and Against Nicaragua (*Nicar. v. U.S.)*, 1986 I.C.J. 14.
– *Carta de Naciones Unidas*, 26 de junio de 1945.
– *Cybersecurity Policy Making as a turning point. Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, OECD, 2012 (http://www.oecd-ilibrary.org/science-and-technology/cybersecurity-policy-making-at-a-turning-point_5k8zq92vdgtl-en)
– *Estrategia de Seguridad Nacional. Un Proyecto Compartido*, Presidencia del Gobierno, 2013.
– *Estrategia Española de Seguridad. Una responsabilidad de todos*, Gobierno de España, 2011.
– *Plan de ciberseguridad de la UE para proteger una red abierta plena de libertad y de oportunidades en línea*, Comisión Europea, 2013, (http://europa.eu/rapid/press-release_IP-13-94_es.htm).
– *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation*, (http://www.nato.int).
– *Strategy for Operating in Cyberspace*, Department of the Army, 2011 (http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/ResenaEstrategiaoperacionesCiberespacio_julio2011.pdf).
– *XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja* (http://www.icrc.org/spa/index.jsp).
– BROAD W.J., MARKOFF J. y SANGER D. E., "Israel Tests on Worm Called Crucial in Iran Nuclear Delay", *New York Times*, 15 de enero de 2011.

– FILDES J., *Stuxnet Virus Targets and Spread Revealed*, BBC NEWS, 15 de febrero de 2011, en: http://www.bbc.co.uk/news/technology- 12465688.
– GALDON CLAVELL, G., "Big Data y miopía de la Administración", *El País*, 19 de marzo de 2013.
– HARARI, H., "Tecnology may endager democracy", *What *should* we be worried about?*, Annual question 2013 (http://edge.org/response-detail/23835).
– MOROZOV, E., "Smart", *what *should* we be worried about?*, Annual question 2013 (http://edge.org/response-detail/23829).
– SCHNEIER, B., "Power and the Internet", *What *should* we be worried about?*, Annual question 2013 (http://edge.org/response-detail/23818).