El presente número monográfico dedicado a la Seguridad y la Defensa, a través de reflexiones provenientes de especialistas civiles y militares, desde un enfoque jurídico, no pretende agotar ninguno de los temas abordados, sino contribuir a la sensibilización sobre la necesidad de abordar investigaciones profundas, en todos los campos del saber, que ayuden a instaurar una sólida cultura de seguridad y defensa en la sociedad española, propia de las democracias más avanzadas del mundo. Su instauración redundará, sin lugar a dudas, en la adopción de medidas de prevención y respuesta, proporcionadas y legítimas, de conformidad con los principios y valores democráticos sobre los que se cimienta nuestra Constitución.

María Susana De Tomás Morales
Directora del Departamento de Derecho Público
Facultad de Derecho (ICADE)

HACIA UNA CULTURA DE CIBERSEGURIDAD: CAPACITACIÓN ESPECIALIZADA PARA UN "PROYECTO COMPARTIDO". ESPECIAL REFERENCIA AL ÁMBITO UNIVERSITARIO

Autor: *Susana De Tomás Morales*[1]
Profesora Propia Agregada. Directora del Departamento de Derecho Público. Coordinadora del Área de Derecho Internacional Público y Relaciones Internacionales. Facultad de Derecho (ICADE). Universidad Pontificia Comillas.

Resumen

La consecución de una cultura de ciberseguridad no es posible a través de acciones de divulgación, aún cuando son necesarias, sino que requiere de una ingente labor formativa especializada que tenga en cuenta en ese proceso de enseñanza/aprendizaje a todos los sectores de la sociedad. Se requiere instaurar una cultura de ciberseguridad inserta en una cultura de seguridad y defensa para implicar en ella a toda la sociedad. Resulta necesario analizar, previamente, los elementos clave sobre los que cimentar una sólida cultura de seguridad y defensa

[1] stomas@der.upcomillas.es

y, posteriormente, abordar la capacitación especializada en ciberseguridad, especialmente en el ámbito universitario.

Palabras clave: Estrategia de Seguridad Nacional; Cultura de Seguridad y Defensa; cultura de ciberseguridad; adiestramiento/capacitación especializada; ámbito universitario y castrense; elementos claves.

Culture of cybersecurity: Training / specialized training for a "shared project". Special reference to University.

Abstract:

The achievement of a culture of cybersecurity is not possible through dissemination actions, even when necessary, but requires a huge specialized training work that takes into account in the process of teaching / learning to all sectors of society. It requires building a culture of cybersecurity inserted into a culture of safety and defense to involve in it the whole society. It is necessary to analyze previously key elements that build a strong culture of security and defense and then attend the specialized training in cybersecurity, especially at the university level.

Key words: National Security Strategy; security and defense culture; culture of cybersecurity; training / specialized training; universitary level and military training; Key elements.

Recibido: 30-04-2014
Aceptado: 22-05-2014

1. ESTRATEGIA DE SEGURIDAD NACIONAL Y FOMENTO DE UNA CULTURA DE SEGURIDAD Y DEFENSA COMO CIMIENTO BÁSICO DE UNA CULTURA DE CIBERSEGURIDAD

A pesar de las posibilidades de desarrollo personal y profesional que nos brinda el ciberespacio, la amenaza cibernética ocupa un lugar destacado entre los riegos y amenazas que atenazan la seguridad interna e internacional. Una respuesta eficaz frente a la amenaza cibernética no es posible si no se consigue la implicación de todos los sectores de la sociedad, a través de una cultura de ciberseguridad. Sin embargo, consideramos que ésta no puede ser atendida de forma aislada, sino como parte integrante de una más amplia cultura de seguridad y defensa. Consecuentemente, consideramos necesario realizar, en primera instancia, una reflexión sobre

cuáles serían las premisas básicas para que se arraigue en la sociedad una sólida cultura de seguridad y defensa. Además de atender a los elementos necesarios para su consecución, se tendrá presente a la Estrategia de Seguridad Nacional de 2013, para poder dilucidar si la misma constituye, a su vez, un elemento facilitador para el arraigo de una cultura de seguridad y defensa en la sociedad española.

Si bien el establecimiento de una cultura de seguridad y defensa requiere la implicación de toda la sociedad en general para hacer frente a los distintos riesgos y amenazas que acechen a la seguridad nacional interna e internacional, se hace aún más necesaria frente a las ciberamenazas. Por ello, extrapolando los elementos necesarios para la consecución de una cultura de seguridad y defensa en general, abordaremos, mediante un análisis deductivo, las premisas básicas que han de ser atendidas en una específica cultura de ciberseguridad.

La consecución de una cultura de ciberseguridad no es posible a través de meras acciones de divulgación, aún cuando éstas sean necesarias, sino que requiere de una ingente labor formativa especializada que tenga en cuenta en ese proceso de enseñanza/aprendizaje a todos los sectores de la sociedad. Sin embargo, esta cultura de ciberseguridad no puede ser eficaz si no se inserta dentro de una cultura de seguridad y defensa. La sucesivas estrategias de seguridad adoptadas por España tienden la mano a la sociedad española para implicarla en la seguridad y defensa de España, bien a través de recordar la corresponsabilidad de la ciudadanía en garantizar la seguridad de nuestro Estado, bien a través de implicarla en un proyecto compartido. No obstante, el grado de implicación de la sociedad dependerá del grado de arraigo que se obtenga de una cultura de seguridad y defensa.

Consecuentemente, resulta necesario realizar una reflexión sobre algunas de las premisas básicas sobre cómo conseguir una implicación de los distintos sectores de la sociedad española frente a la amenaza cibernética. Si bien toda la sociedad en su conjunto debe implicarse en una cultura de ciberseguridad, el ámbito universitario debe abordar esta importante cuestión, en cuanto a su función de servicio a la sociedad. Por ello, en último lugar, se esbozarán unas breves notas, a modo de reflexiones en voz alta, sobre cuál es el papel que deberían jugar las instituciones universitarias para conseguir un sólido arraigo de una cultura de ciberseguridad, tanto en relación con la sociedad en general, como en relación con determinados sectores, en particular.

1.1. La Estrategia de Seguridad Nacional instrumento clave para una cultura de seguridad y defensa

El primer punto de partida se debe centrar en cómo las estrategias de seguridad de España tienen en consideración a la sociedad española y si constituyen un eficaz instrumento para la consecución de una conciencia de cultura de ciberseguridad, cimentada en una cultura de seguridad y defensa.

El pasado día 31 de mayo de 2013, el Consejo de Ministros aprobó la nueva estrategia de seguridad de España, bajo el título "Estrategia de Seguridad Nacional. Un proyecto compartido"[2] (en adelante, ESN), en la que se incorpora una visión renovada y reforzada de la seguridad interna e internacional en relación con la establecida en 2011. Esta nueva visión viene reflejada ya en la propia denominación de la nueva estrategia de seguridad española con la introducción de importantes cambios terminológicos sobre los que, con carácter previo, resulta necesario reflexionar a fin de averiguar si los mismos pueden ser considerados como elementos favorecedores de una cultura de defensa.

Si bien la estrategia de seguridad de 2011, bajo el título "Estrategia Española de Seguridad. Una responsabilidad de todos"[3] (en adelante, EES), hacía un llamamiento a la necesaria contribución de la sociedad en su conjunto para preservar la seguridad ante nuevos riesgos y amenazas, estableciendo, acertadamente, que la responsabilidad de la seguridad española no sólo debía reposar en el Gobierno y en las Administraciones públicas, sino que era extensible a toda la sociedad, presentaba algunas carencias que la nueva versión del 2013 corrige y muestra en su nuevo título.

La EES de 2011 obviaba el término "nacional", omitiendo, así, uno de los primeros elementos esenciales para conseguir una cultura de seguridad y defensa integradora de toda la sociedad española. Por lo tanto, no puede entenderse una estrategia española de seguridad sin dirigir su mirada hacia la Nación española. No debemos olvidar, tal y como se establece en el Preámbulo de nuestro texto constitucional, que fue la Nación española quien proclamó su voluntad de:

> *"Garantizar la convivencia democrática dentro de la Constitución y de las leyes conforme a un orden económico y social justo;*
> *Consolidar un Estado de Derecho que asegure el imperio de la ley como expresión de la voluntad popular;*
> *Proteger a todos los españoles y pueblos de España en el ejercicio de los derechos humanos, sus culturas y tradiciones, lenguas e instituciones;*
> *Promover el progreso de la cultura y de la economía para asegurar a todos una digna calidad de vida;*
> *Establecer una sociedad democrática avanzada, y*
> *Colaborar en el fortalecimiento de unas relaciones pacíficas y de eficaz cooperación entre todos los pueblos de la Tierra".*

[2] *Estrategia de Seguridad Nacional. Un proyecto compartido*. Presidencia del Gobierno, 2013. Documento disponible en la siguiente página web: http://www.lamoncloa.gob.es/nr/rdonlyres/d0d9a8eb-17d0-45a5-adff-46a8af4c2931/0/estrategiaespanoladeseguridad.pdf

[3] *Estrategia Española de Seguridad. Una responsabilidad de todos*. Gobierno de España, 2011. Documento disponible en la siguiente página web : http://www.lamoncloa.gob.es/nr/rdonlyres/d0d9a8eb-17d0-45a5-adff-46a8af4c2931/0/estrategiaespanoladeseguridad.pdf

Por otra parte, el artículo 2 de la Constitución española (en adelante, CE) establece que nuestro texto constitucional tiene su fundamento en la indisoluble unidad de la Nación española, que es definida como *"patria común e indivisible de todos los españoles"*. Ignorar a la Nación española tiene unas consecuencias negativas para el establecimiento de una sólida y eficaz cultura de seguridad y defensa en España, a diferencia de lo que ocurre en otros Estados con sus respectivas estrategias de seguridad nacional. Esto se debe a que del grado de conciencia nacional depende el grado de conciencia de defensa y, consecuentemente, repercute en el grado de cultura de seguridad y defensa de un Estado, tal y como ilustra CONDE DE ARJONA[4] al realizar un análisis comparado entre cinco Estados (Israel; Italia; Chile; Argentina; Francia y Reino Unido), atendiendo al grado de incidencia de esos tres conceptos clave: conciencia nacional - conciencia de defensa - cultura de seguridad y defensa.

Es evidente que hubiese sido deseable el que la EES de 2011 hubiese incluido el término "nacional". Sin embargo, la EES establecía que "garantizar la seguridad de España y de sus habitantes y ciudadanos" es también responsabilidad de la ciudadanía. Podemos entrever, de forma indirecta, la responsabilidad que el pueblo español asumió al ratificar la CE, en cuyo artículo 30.1 se establece que *"los españoles tienen el derecho y el deber de defender a España"*. Más allá de una falta de valentía para impulsar expresamente una conciencia nacional y una conciencia de defensa, no debemos minusvalorar este importante documento que fue elaborado al mismo tiempo en que adoptaban estrategias nacionales otros Estados, así como en el ámbito de la OTAN, y que, como señala ARGUMOSA[5], nos ha permitido incluirnos en el "selecto club" del reducido grupo de democracias avanzadas que cuentan con una moderna estrategia de seguridad nacional.

Por su parte, la ESN de 2013 actualiza y refuerza la estrategia española de 2011, indicando de forma expresa en su título que es la estrategia de seguridad propia de la Nación española. Además, la ESN se presenta como un proyecto compartido y no sólo se hace una somera mención a que es responsabilidad de toda la sociedad el garantizar la seguridad de España, sino que es incluido, como principio informador de la ESN, el concepto de responsabilidad compartida bajo el lema "Unidad de acción". La inclusión de este principio se justifica debido al *"enfoque integral de la seguridad, comprensivo de todas sus dimensiones"*, lo que precisa de una gestión completa a través de un Sistema de Seguridad Nacional en el que participe activamente la sociedad en general y con un reforzamiento de la colaboración público-privada.

[4] CONDE DE ARJONA, J., "La Cultura de Seguridad y Defensa en los países de nuestro entorno", en *Cuadernos de Estrategia* núm. 155 (Ejemplar dedicado a: *La Cultura de Seguridad y Defensa. Un proyecto en marcha*), IEEE, Ministerio de Defensa, Madrid, 2011, pp. 104-140.

[5] ARGUMOSA, J., "Una estrategia moderna de seguridad nacional", en Revista *Política Exterior*, Vol. 24, núm. 138. noviembre-diciembre 2010, pp. 80-90.

Sin embargo, ¿cómo se puede compartir un proyecto si no existe una cultura de seguridad y defensa arraigada en la sociedad? ¿Es consciente la sociedad española de las grandes transformaciones que han sufrido los conceptos de seguridad y defensa y por qué es necesaria su implicación? En concreto, ¿Es consciente de las consecuencias de las amenazas cibernéticas y de su necesaria implicación?

La ESN se presenta desde un enfoque integral de la seguridad nacional, 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 clásica defensa del territorio a la estabilidad económica y financiera o la protección de las infraestructuras críticas. Según la ESN, la seguridad es considerada como

> *un fundamento esencial para el desarrollo y el progreso de una sociedad libre. Por eso resulta imprescindible un entendimiento básico y generalizado de la importancia de la seguridad como garantía de bienestar de los ciudadanos y de la estabilidad del propio Estado".*

Se requiere, por lo tanto, una labor de formación básica homogénea y accesible a toda la sociedad para que se arraigue en la sociedad una verdadera cultura de seguridad y defensa propia de todas las sociedades democráticas avanzadas, así como un adiestramiento/capacitación especializada en relación con las amenazas cibernéticas que puede sufrir cualquier ciudadano.

1.2. Cultura de seguridad y defensa como cimiento de una cultura de ciberseguridad

La EES, adoptada en 2011, introdujo el concepto de visión integral de la seguridad, que es reforzada en la ESN. Ante esta renovada visión integral de la Seguridad Nacional, acertadamente se establece, en 2013, que

> *"Una sociedad responsable y concienciada de su seguridad está en mejores condiciones para hacer frente a los desafíos actuales y ganar en términos de desarrollo y prosperidad [...]"* por lo que se considera *"esencial promover la participación del ciudadano y la colaboración público-privada [...]".*

Consecuentemente, la implicación de la sociedad civil (especialmente en los ámbitos de interés prioritario de la Seguridad Nacional) y el fomento de la cultura de defensa constituyen uno de los ocho principios sobre los que se sustenta nuestro Sistema de Seguridad Nacional.

En esta nueva versión de la estrategia de Seguridad nacional, desaparece la clásica división entre seguridad nacional interna y exterior, ofreciendo una novedosísima definición de Seguridad Nacional:

> *"acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos".*

El gran reto que se plantea consiste en cómo conseguir que la sociedad española sea una sociedad responsable y concienciada de su seguridad. La solución sería arraigar en la sociedad una cultura de seguridad y defensa. Sin embargo, como ya se ha indicado, sería necesario que existiese una conciencia nacional y una conciencia de defensa. CONDE DE ARJONA ofrece unas sencillas e ilustrativas definiciones que nos servirán de base para un posterior desarrollo de las mismas. Así, este autor indica que la conciencia nacional debe ser entendida como "el amor al propio país"[6] y la conciencia de defensa como "el valor que nos merece aquello que tenemos, llámese planeta, nación, o sin ánimo de trivializar, club deportivo", pues "[...] una vez valoramos lo que poseemos, analizamos las posibles amenazas o riesgos que le acechan o pueden acechar"[7].

El amor por el propio Estado o conciencia nacional implicaría el sentimiento común de la sociedad por valorar la posición de España desde una perspectiva histórica, desde su constitución como Estado y recordando su protagonismo en la primogénita Sociedad Internacional - La Sociedad Internacional de Estados Europeos -, pasando por momentos de claroscuro, hasta la España actual, la España inmersa en una democracia avanzada y lo que ello representa. ¿Acaso no hay motivos de orgullo y de sentimientos positivos hacia nuestro Estado? A partir de ahí, podremos valorar lo que poseemos y podremos entender la definición de Seguridad Nacional que nos ofrece la ESN. Si se carece de una conciencia nacional, es difícil implicar a la sociedad en defender los valores que ello conlleva. Por otra parte, una cultura de defensa nos llevaría a preguntarnos: ¿Sabemos valorar nuestros principios y valores constitucionales? ¿estaríamos dispuestos a defenderlos frente a las amenazas y riesgos que los acechan? La respuesta a estos interrogantes tiene un punto en común: la necesaria formación de la sociedad en los principios y valores constitucionales - destacando los valores superiores de igualdad, justicia, libertad y pluralismo político enunciados en el art.1.1 CE- que nos permiten disfrutar de un Estado social y democrático de Derecho.

Desde esta perspectiva podemos entender que la defensa de España no se limita a las respuestas que, ante determinados riesgos y amenazas, deban ofrecerse desde el ámbito militar. Al contrario, la evolución del concepto de seguridad, que incluso ha llegado a difuminar la línea divisoria entre seguridad nacional interna

[6] CONDE DE ARJONA, J., La Cultura de Seguridad y Defensa ..., op. cit. en cita 4 *supra*; p. 107.

[7] *Ibidem*, p. 113.

e internacional[8], requiere la participación de toda la sociedad frente a las amenazas y riesgos que ponen en peligro nuestros principios y valores constitucionales, nuestro Estado social y democrático de Derecho y la propia supervivencia del Estado español. Esta nueva visión integral de la seguridad, no reduccionista a los riesgos militares que exigen evidentes respuestas desde el ámbito de la Defensa, se introdujo ya en la EES de 2011, al establecer que afrontábamos

> *"amenazas y riegos transversales, interconectados y transnacionales. Preservar la seguridad requiere coordinación, tanto internacional como interna, y la contribución de la sociedad en su conjunto".*

La ESN reafirmará la visión integral y transversal de la seguridad nacional interna e internacional. Consecuentemente, se requiere una capacitación especializada de la sociedad en general sobre los riesgos y amenazas que desde una visión integral y transversal nos ofrece la ESN.

1.2.1. La atención a los riesgos y amenazas en una cultura de seguridad y defensa

La ESN atiende a los riesgos y amenazas ofrecidos en la versión de 2011 (conflictos armados, terrorismo, crimen organizado, inestabilidad económica y financiera, vulnerabilidad energética, proliferación de armas de destrucción masiva, ciberamenazas, flujos migratorios irregulares; emergencias y catástrofes), añadiendo tres nuevos (espionaje, vulnerabilidad del espacio marítimo, en sentido amplio, y vulnerabilidad de las infraestructuras críticas y servicios esenciales). A partir de los mismos, se indican doce ámbitos prioritarios de actuación. Dentro de cada uno, se delimita cuál es el objetivo principal a alcanzar, así como varias líneas de actuación concretas. Además de estos riesgos y amenazas, tanto en la versión de 2011 como en la actual, se intenta dar un tratamiento integral de la seguridad, atendiendo a factores potenciadores que pueden generar nuevos riesgos o amenazas o multiplicar o agravar efectos (pobreza; cambio climático; desequilibrios demográficos; extremismos ideológicos; la generalización del uso nocivo de las tecnologías; así como las desigualdades), aunque, a diferencia de su predecesora, la ESN no procede a un desarrollo expreso y autónomo de cada factor potenciador, sino que son atendidos desde un enfoque transversal e integral al atender las respectivas amenazas y riesgos.

[8] La EES de 2011 ya establecía que *"los límites entre la seguridad interior y la seguridad exterior se han difuminado. Las políticas nacionales en los ámbitos tradicionales de la seguridad ya no son suficientes para salvaguardarla en el siglo XXI"*. Por su parte, de forma novedosa, como se ha indicado, la ESN nos ofrecerá una definición única de seguridad nacional interna e internacional.

1.2.2. La globalización de los riesgos y amenazas y su necesaria respuesta colectiva

La novedosa definición de seguridad nacional interna e internacional que ofrece la ESN no olvida la dimensión global de determinados riesgos y amenazas, que no pueden ser atendidas de forma adecuada desde respuestas estatales unilaterales. De ahí, la necesidad de *"contribuir junto a nuestros socios y aliados a la seguridad internacional"*. Esta dimensión global de la seguridad ya fue atendida en la EES al entender que España tiene *"intereses globales que defender y amenazas y riesgos transnacionales que afrontar"*. En este sentido, GONZÁLEZ CUSSAC señalaría que

> "[...] parece claro que la categoría de seguridad nacional se construye ya hoy desde una perspectiva multidimensional: militar, política, económica, social (identitaria) y medioambiental. Es decir, como equivalente a exención de peligro, daño o riesgo en todos estos ámbitos, y por tanto entendida como seguridad colectiva, compartida y global"[9]

Por su parte, AVILÉS FARRÉ afirmaría que:

> "[...] la globalización y el progreso tecnológico que la acompaña modifican las coordinadas de la seguridad por la creciente interdependencia de los Estados en todos los campos, incluida la defensa, por la proliferación de las amenazas transnacionales en el ámbito de la justicia e interior y por la creciente internacionalización de otros riesgos"[10]

Es evidente que el proceso de globalización, más allá de sus evidentes y ya conocidos efectos positivos, también se ha convertido en un instrumento facilitador o agravante de riesgos y amenazas para la seguridad y la defensa, adquiriendo una nueva dimensión global. Esta nueva dimensión hace necesario el articular estrategias de seguridad y defensa globales a través de una apuesta por el multilateralismo. No debemos olvidar que desde el ámbito de las Naciones Unidas ha quedado claramente establecido que un orden internacional democrático y equitativo requiere, entre otras cosas, de:

> "La responsabilidad compartida entre las naciones del mundo de gestionar el desarrollo económico y social a nivel mundial y de hacer frente a las

[9] GONZÁLEZ CUSSAC, J.L., "Estrategias legales frente a las ciberamenazas", en *Cuadernos de Estrategia*, núm. 149, (Ejemplar dedicado a: *Ciberseguridad. Retos y amenazas a la ciberseguridad en el ciberespacio*), IEEE, Ministerio de Defensa, Madrid, 2011, pp. 83-127.

[10] AVILÉS FARRÉ, "Por un concepto amplio de seguridad", en AA.VV., *Revisión de la Defensa Nacional* núm. 55 de la colección Monografías del Centro Superior de Estudios de la Defensa Nacional, Madrid, 2002, p. 20.

amenazas contra la paz y la seguridad internacionales, que debe ser ejercida multilateralmente"[11]

En efecto, como se indicaba en el Informe *"Un mundo más seguro: la responsabilidad que compartimos"*[12], elaborado por el Grupo de alto nivel sobre las amenazas, los desafíos y el cambio[13], en el Siglo XXI, aunque los Estados soberanos deben seguir asumiendo un protagonismo principal en la lucha contra antiguas y nuevas amenazas, resulta imposible dar una respuesta eficaz de forma aislada, por lo que resulta *"indispensable contar con estrategias colectivas, instituciones colectivas y un sentido de responsabilidad colectiva"*, debido a la confluencia de *"tres pilares básicos"*: 1) el carácter transfronterizo de las amenazas, íntimamente relacionadas entre sí, requieren respuestas coordinadas a nivel mundial, regional y nacional; 2) Más allá de sus capacidades, ningún Estado en solitario puede hacerse "invulnerable" a las nuevas amenazas; y 3) No se puede dar por supuesto que todos los Estados cumplan con sus obligaciones internacionales, tanto en relación con otros Estados como en relación con la protección de su propia población. La necesidad de buscar un nuevo consenso en materia de seguridad, sería asumido, en 2005, por el entonces Secretario General de las Naciones Unidas, Kofi A. Annan a través de su conocido informe *"Un concepto más amplio de la libertad: desarrollo, seguridad y derechos humanos para todos"*[14].

Asumiendo la globalización de los riesgos y amenazas y la necesidad de ofrecer una respuesta colectiva, multidimensional y multilateral, el capítulo segundo de la ESN, bajo el título "La seguridad de España en el mundo", atiende a la seguridad internacional en el contexto de un mundo globalizado, competitivo y en constante proceso de cambio. Entre los entornos estratégicos que se incluyen en la ESN vamos a atender a dos de ellos: el ámbito universal de la Organización de las Naciones Unidas (en adelante, ONU) y el regional de la Unión Europea (en adelante, UE).

En relación con el primero de los ámbitos, se reconoce el papel que juega la ONU para ofrecer soluciones globales ante los retos y amenazas globales, siendo considerada *"la organización más relevante para la cooperación mundial y el mantenimiento de la paz y la seguridad internacional"*. En cuanto al ámbito de la UE, se recuerda el compromiso de España en relación con dos grandes objetivos de la

[11] Resolución "Promoción de un orden internacional democrático y equitativo" aprobada por la Asamblea General el 18 de diciembre de 2013. Doc. A/RES/68/175.

[12] Informe del Grupo de alto nivel sobre las amenazas, los desafíos y el cambio: *"Un mundo más seguro: la responsabilidad que compartimos"*. Doc. A/59/565, de 2 de diciembre de 2004.

[13] Este Grupo fue creado a iniciativa del Secretario General de las Naciones Unidas, tal y como lo anunció, en 2003, ante la Asamblea General. Doc. A/58/612.

[14] Informe del Secretario General: *"Un concepto más amplio de la libertad: desarrollo, seguridad y derechos humanos para todos"*. Doc. A/59/2005.

Unión que *"comparte e impulsa"*: la integración política y el fortalecimiento de mecanismos eficaces de gobernanza económica y financiera. Todo ello bajo el firme convencimiento de que *"avanzar en la construcción europea es aval de más seguridad y prosperidad para España"*.

Atendiendo a estos dos ámbitos, se debe reflexionar sobre su incidencia en una cultura de seguridad y defensa desde un enfoque global. Si el arraigo de una cultura de seguridad y defensa depende del grado de conciencia nacional y de conciencia de defensa, avanzar en una moderna concepción de cultura de seguridad y defensa requiere extender ambos conceptos hacia un nuevo y renovado concepto de seguridad que engloba tanto la seguridad interna como la internacional.

La conciencia nacional y la conciencia de defensa debe atender consecuentemente el "amor" al propio Estado y al ámbito organizativo internacional del que forma parte España. Si bien el "amor" hacia el propio Estado puede surgir desde un movimiento espontáneo, el "amor" hacia Organizaciones Internacionales que la población percibe como distantes y ajenas a su propia realidad e identidad, requiere de un proceso más largo para llegar a amarlas. Sin embargo, con independencia de cuál sea el desencadenante del chispazo de "amor", lo importante es que todo amor crece y madura con el conocimiento del amado, por lo que se requiere una labor de sensibilización de la población hacia esa realidad de nuestro entorno estratégico para despertar sentimientos de "amor", mediante una formación/capacitación en el ámbito de las Organizaciones Internacionales. Esta actividad pedagógica ha de dirigirse a toda la población en general, de tal manera que se arraigue en la población un sentimiento común de ser ciudadano español, ciudadano europeo y ciudadano del mundo. Desde esa labor no meramente divulgativa sino formativa, se podrá avanzar en el arraigo de una conciencia nacional, regional y universal, acorde con el nuevo concepto de seguridad nacional interna e internacional. A partir de entonces, se podrá valorar lo que tenemos desde una dimensión interna e internacionalmente. Es decir, desarrollar una cultura de defensa, en el sentido de generar sentimientos positivos en la población de que merece la pena defender lo que tenemos. Si bien en relación con la conciencia nacional y la conciencia de defensa era importante tener como referente los principios y valores constitucionales, se requiere, en especial, una importante labor formativa sobre los principios y valores que compartimos en el ámbito internacional para generar sentimientos de "amor" hacia los mismos (podríamos también hablar de sentimientos de aceptación de los mismos como propios) y así poder valorarlos (generar sentimientos positivos hacia la defensa de los mismos: merece la pena defenderlos en nuestro Estado y en cualquier parte del mundo).

Atendiendo a los dos ámbitos organizativos seleccionados, podemos apreciar cómo los principios y valores incluidos en la CE se encuentran en sintonía con los principios y valores que, en materia de seguridad, se acogen en las Organizaciones Internacionales de referencia de las que España es Estado miembro. Además, la

estrecha cooperación en materia de seguridad entre ambas Organizaciones Internacionales refuerza la necesaria cooperación y multilateralismo para hacer frente a los riesgos y amenazas que ponen o puedan poner en peligro la seguridad nacional interna e internacional.

La opción por el multilateralismo, incluida tanto en la EES como en la actual ESN, debe situarse en una acción coherente de cumplimiento de los compromisos internacionales asumidos por España. No debemos olvidar que entre los fines y objetivos de las Naciones Unidas se encuentra el mantenimiento de la paz y seguridad internacionales, por lo que se establece, en el artículo 1.1 de la Carta de las Naciones Unidas (en adelante, Carta), el deber de *"tomar medidas colectivas eficaces para prevenir y eliminar las amenazas a la paz y para suprimir actos de agresión u otros quebrantamientos de la paz"*. Para el cumplimiento de este deber se articula todo un Sistema de Seguridad Colectivo que incluye tanto acciones colectivas preventivas, dirigidas al arreglo pacífico de controversias, como acciones colectivas de respuesta en caso de amenazas a la paz y la seguridad internacionales (tanto a través de medidas recomendatorias y coercitivas, incluidas, respectivamente, en los Capítulos VI y VII de la Carta), en el que las Naciones Unidas asumen un indiscutible liderazgo, pero no un monopolio en materia de seguridad. Al contrario, tanto en relación con las medidas adoptadas en el seno de las Naciones Unidas, en relación con acciones concretas a desarrollar en virtud de los Capítulos VI y VII de la Carta, las Organizaciones Internacionales regionales adquieren cada vez un mayor protagonismo que repercute en una mayor eficacia del Sistema de Seguridad Colectivo. Sin embargo, será a través del Capítulo VIII de la Carta donde se desarrollará un Sistema de Seguridad Colectivo basado en la cooperación y el multilateralismo entre las Naciones Unidas y las Organizaciones Regionales[15].

[15] Será a partir de la década de los 90 cuando proliferen las Resoluciones del Consejo de Seguridad de las Naciones Unidas, en virtud del Capítulo VIII de la Carta, en las que se tiene en consideración a las Organizaciones Internacionales de ámbito regional en el campo de la prevención y resolución de conflictos. No obstante, podemos destacar algunos grandes hitos en el ámbito de la Organización que han propiciado una colaboración y cooperación más estrecha con las Organizaciones Regionales: En 1992, el Secretario Nacional de las Naciones Unidas, en su Informe "Un programa para la Paz", hacía un llamamiento a la implicación de las Organizaciones Internacionales regionales para que se vinculasen a los mecanismos de las Naciones Unidas, a través de distintas esferas de acción: diplomacia preventiva, establecimiento, mantenimiento y consolidación de la paz (*Vid. doc:* "Un programa de paz: diplomacia preventiva, establecimiento de la paz y mantenimiento de la paz", Informe del Secretario General presentado de conformidad con la declaración aprobada el 31 de enero de 1992 en la Reunión en la Cumbre del Consejo de Seguridad, de 17 de junio de 1992. Doc: S/24111). Este Informe llevaría a la Asamblea General de las Naciones Unidas a reflexionar sobre cómo mejorar esta cooperación (*Vid. doc.: Declaración sobre el mejoramiento de la cooperación entre las Naciones Unidas y los acuerdos u organismos regionales en el mantenimiento de la paz y la seguridad internacionales*, Resolución 49/57 de la Asamblea General de las Naciones Unidas, adoptada el 9 de diciembre de 1994. Doc: A/RES/4957 /1994). Las esferas de acción se reforzarían, en 1995, una vez más de manos de Butros Gali, con un Suplemento al referido programa, incorporando instrumentos dirigidos al desarme, al establecimiento de sanciones y de imposición de la paz. De especial relevancia, en el contexto del presente artículo, será su llamamiento a las Organizaciones

De especial interés, atendiendo a los dos ámbitos organizativos que, a modo de ejemplo, hemos seleccionado para atender a la dimensión global de la seguridad y la articulación de un sistema colectivo de seguridad mediante la cooperación y el multilateralismo, podemos señalar, siguiendo a BLANC ALTEMIR, que si bien las Naciones Unidas debe seguir ejerciendo un liderazgo en relación con los grandes retos a los que se enfrenta la Sociedad Internacional actual, no hay que olvidar que

> " [...] la UE ha promovido y continúa contribuyendo de forma intensa a la construcción y mejora del sistema multilateral que representan las Naciones Unidas, entre otras razones porque el multilateralismo está en su propio ADN"[16].

Ambas Organizaciones Internacionales comparten unos valores comunes, forjando

> "[...] una progresiva cooperación e intensificación de sus relaciones inspiradas por una concepción también compartida del multilateralismo y su capacidad de dar respuestas a escala universal o regional a los múltiples retos y amenazas que afronta la comunidad internacional"[17]

Con estas premisas de partida se podrá desarrollar una cultura de seguridad y defensa, atendiendo a una perspectiva multidimensional de la seguridad, es decir, reflexionar sobre los posibles riegos y amenazas que pongan en peligro a la seguridad de España interna e internacional. En concreto, la ESN no sólo incluye dentro de su entorno estratégico a los ámbitos regionales de las Naciones Unidas y de la UE, sino que, además, su visión multidimensional y multilateral

regionales, incluso si su ámbito preferente de competencias no es el de la seguridad y la defensa, como son las Organizaciones preferentemente económicas, o de fines político sociales (*Vid. doc.: Suplemento de "Un programa de paz"*, Documento de posición del Secretario General presentado con ocasión del cincuentenario de las Naciones Unidas, de 25 de enero de 1995. Doc: S/1995/1). En el año 2000, dos documentos clave: el conocido Informe Brahimi (*Vid. doc.: "Informe Brahimi" o Informe del Grupo sobre Operaciones de Mantenimiento de la Paz de las Naciones Unidas*. Doc: A/55/305-S/2000/809) y la llamada "Declaración del Milenio" de la Asamblea General (*Vid.doc.:* Resolución 55/2 de la Asamblea General, adoptada el 13 de septiembre de 2000. Doc: A/RES/55/2). En 2005, la Cumbre Mundial reforzó la cooperación de las Organizaciones regionales en la labor del Consejo de Seguridad (*Vid. doc.: Documento Final de la Cumbre Mundial 2005*. Doc:A/RES/60/1) . Este órgano, recogió ese propósito en la Resolución 1631(*Vid. doc.* Resolución 1631, adoptada por el Consejo de Seguridad en su 5282ª sesión, celebrada el 17de octubre de 2005- Doc. S/RES/1631 (2005). A partir de 2005 se irá reforzando la cooperación entre las Organizaciones regionales y las Naciones Unidas hasta la actualidad.

[16] BLANC ALTEMIR, A., "Introducción: Las Naciones Unidas y la Unión Europea: valores y ámbitos de acción compartidos en aras de una multilateralismo más eficaz", en BLANC ALTEMIR, A. (Dir.), *Las relaciones entre las Naciones Unidas y la Unión Europea. Seguridad, Cooperación y Derechos Humanos*, Ed. Tecnos, Madrid, 2013, p. 20.

[17] *Ibidem*, p. 24.

se extiende al Mediterráneo, a América Latina, a Estados Unidos y la relación transatlántica, a África, a Asia, a Australia, a Rusia y a la OTAN, así como a otros foros multilaterales. La seguridad de España en el mundo es considerada como un objetivo primordial y es objeto de desarrollo en el capítulo segundo de la ESN. Consecuentemente, para conseguir arraigar en la sociedad española una sólida cultura de seguridad y defensa no debe obviarse la dimensión internacional de la seguridad y de la defensa desde el contexto del multilateralismo.

1.2.3. Enfoque transversal de los riegos y amenazas

A partir del establecimiento de una conciencia nacional en una dimensión internacional y con una conciencia de defensa, en sentido amplio, se debe desarrollar una sólida cultura de seguridad nacional interna e internacional y de defensa a través del conocimiento de las amenazas y riesgos que la acechan. El conocimiento y consecuentemente, la labor formativa que conlleve a su conocimiento, necesita, además, no ignorar el enfoque transversal con el que han de ser abordados los referidos riesgos y amenazas. De esta manera podremos entender de qué debemos defendernos y por qué es necesaria la implicación de toda la sociedad en general.

La ESN destina su capítulo tercero al análisis de los riesgos y amenazas para la Seguridad Nacional, sin dejar de atender a los factores potenciadores que pueden desencadenarlos o agravarlos. En relación con los riesgos y amenazas, mantiene los ocho introducidos en la EES, a saber: los conflictos armados; el terrorismo; el crimen organizado; la inestabilidad económica y financiera; la vulnerabilidad energética; la proliferación de armas de destrucción masiva; las ciberamenazas; los flujos migratorios irregulares; y las emergencias y catástrofes. Además, introduce tres nuevos: el espionaje; la vulnerabilidad del espacio marítimo, en sentido amplio, y la vulnerabilidad de las infraestructuras críticas y servicios esenciales. El proceso de enseñanza/aprendizaje de los mismos ha de realizarse desde un enfoque integral y transversal de los mismos, de tal forma que no sean atendidos como compartimentos estancos, sino atendiendo a la interconexión entre ellos.

A diferencia de la EES de 2011, en la que se dedicaba un capítulo al desarrollo de los factores potenciadores, la nueva ESN no los obvia, pues son objeto de atención a modo de introducción de los riegos y amenazas contenidos en el capítulo tercero, pero no son objeto de desarrollo. Esta novedad resulta adecuada en el contexto del nuevo enfoque integral y transversal que se les ofrece a los riegos y amenazas, de tal forma que los factores potenciadores deberán ser atendidos en todos y cada uno ellos y, en algunos, conectados entre sí. Una de las cuestiones que no quedaba claramente establecida en la EES era la relativa al carácter exhaustivo o no de los factores incluidos en la misma. Esta cuestión queda resuelta en 2013, pues los factores potenciadores enunciados en la ESN no se presentan como números *clausus*, al indicar que:

"la pobreza, la desigualdad, los extremismos ideológicos, los desequilibrios demográficos, el cambio climático o la generalización del uso nocivo de las nuevas tecnologías son algunos de esos factores".

Al único factor potenciador que dedica una mayor extensión es el cambio climático. Por otra parte, desaparecen, como factor potenciador del riesgo, los denominados *"peligros tecnológicos"* que se incluían en la EES para considerar únicamente los usos nocivos de las nuevas tecnologías. Este cambio viene a corregir las disfunciones que presentaba la EES, pues, como señalaría SERRA REXACH, en relación con los denominados factores potenciadores "... se describen situaciones o actividades que si bien en determinadas circunstancias pueden incrementar los riesgos que tiene la seguridad nacional, en otras ocasiones pueden ser exactamente lo contrario: limitadores del riesgo. Así sucede, por ejemplo, con las nuevas tecnologías, que si ciertamente pueden jugar un papel negativo respecto a la seguridad nacional, pueden también jugarlo positivo"[18].

Al atender a los factores potenciadores, en la ESN se indica, *in fine*, que también han de ser considerados otros elementos como la disfuncionalidad y vulnerabilidad de los Estados fallidos o determinadas actuaciones que pueden afectar a la confianza en las instituciones como *"la capacidad creciente de interferencia de grupos de individuos cuyas actuaciones, como la difusión de información sensible o de rumores de forma indiscriminada, son distorsionadas"*.

En definitiva, podemos concluir que el arraigo de una sólida cultura de seguridad y defensa es imprescindible para la participación de toda la sociedad en general. Sin embargo, no puede enraizar en la sociedad si no se lleva a cabo una labor formativa adecuada de los ciudadanos. Esa cultura de seguridad y defensa debe adecuarse a los profundos cambios acontecidos en los ámbitos de la seguridad y de la defensa.

Las estrategias de seguridad nacionales son un eficaz instrumento que debe guiar el enfoque integral y transversal de los riesgos y amenazas a la seguridad nacional interna e internacional, pero por sí mismos no consiguen el resultado deseado. Como recuerda LABOIRE IGLESIAS,

"las Estrategias de Seguridad Nacional no deben ser consideradas un fin en sí mismo. Estos documentos constituyen una referencia de máximo nivel para llevar a cabo el planteamiento estratégico, que como actividad política comprensiva, conlleva decisiones para resolver el problema de seguridad"[19].

[18] SERRA RESACH, E., Introducción, *Cuadernos de Estrategia* núm. 155, (Ejemplar dedicado a: *La Cultura de Seguridad y Defensa. Un proyecto en marcha*), IEEE, Ministerio de Defensa, Madrid, 2011, p. 11.

[19] LABOIRE IGLESIAS, M., *La Estrategia de Seguridad Nacional (Mayo 2013)*, en Instituto Español de Estudios Estratégicos, Documento de Análisis núm. 34/2013, de 3 de junio de 2013, p. 5.

Para ello se requiere el desarrollo de políticas públicas dirigidas a la formación de la población, desde acciones formativas básicas y homogéneas para toda la sociedad hasta programas de adiestramiento y/o capacitación especializada para determinados sectores de la población.

2. LA NECESARIA IMPLICACIÓN DE TODA LA SOCIEDAD FRENTE A LAS CIBERAMENZAS A TRAVÉS DE UNA CULTURA DE CIBERSEGURIDAD

La necesaria implicación de todos los sectores de la sociedad frente a las ciberamenazas constituye uno de los ejes principales de la ESN, en la que se establece que:

> *"la colaboración y el apoyo del ciudadano son imprescindibles. Esta implicación será posible si se fomenta una cultura de seguridad sólida, basada en el previo conocimiento y sensibilización sobre la importancia que la seguridad reviste para garantizar su libertad, prosperidad y, en suma, su modo de vida conforme a los postulados del Estado social y democrático de Derecho".*

El desarrollo de una sólida cultura de seguridad nacional e internacional, con un enfoque integral y transversal debe cimentar el establecimiento de una cultura de ciberseguridad. Para su consecución, tomando como referencia los parámetros antes atendidos, se hace necesario poder valorar lo que tenemos y tener un sólido conocimiento de los posibles riesgos y amenazas que ponen en peligro o puedan hacer peligrar un modo de vida propios del Estado social y democrático de Derecho. Estas acciones permiten la instauración de una conciencia nacional y conciencia de defensa como requisitos previos e indispensables de una cultura de seguridad y defensa.

Entre los riegos y amenazas contenidos en la ESN se recogen las ciberamenazas como una grave amenaza a la seguridad nacional e internacional, considerada en si misma o en combinación con otros riesgos y amenazas, lo que requiere la implicación de toda la sociedad. La ciberseguridad constituye uno de los principales ámbitos de actuación de la ESN, por su naturaleza transnacional y su interconexión con otros riesgos y amenazas, en un nuevo espacio, el ciberespacio, que facilita su expansión e impacto. Como se indica en la Estrategia, el ciberespacio constituye en la *actualidad "el ejemplo más claro de un ámbito accesible, poco regulado y de difícil control".*

Para que la sociedad en su conjunto pueda implicarse en un "proyecto compartido" frente a las ciberamenazas, se quiere, además, la creación de una conciencia de ciberseguridad, a través de una labor formativa y de sensibilización. Se requiere, pues, atender a las ciberamenazas, desde un enfoque integral, tal

y como se recoge en la ESN. Consecuentemente, se hace necesario incluir en una conciencia de ciberseguridad, el conocimiento de este nuevo espacio, como punto de partida.

En la ESN se atiende al ciberespacio como nuevo ámbito de relación que surge del desarrollo de las nuevas tecnologías de la información y las comunicaciones, diluyendo las fronteras y *"permitiendo una globalización sin precedentes, que propicia nuevas oportunidades, pero conlleva serios riesgos y amenazas".* Lo importante es incluir en una conciencia de ciberseguridad al ciberespacio como otro espacio más junto al espacio terrestre, marítimo y aéreo en que estamos acostumbrados a desarrollar nuestras relaciones personales y profesionales. El conocimiento de este nuevo espacio, tanto en relación con las oportunidades que propicia como los riesgos y amenazas que la acechan resulta vital. El ciberespacio es una realidad que nos acompaña en nuestra vida diaria, pero que ha irrumpido en ella a un ritmo muy acelerado y sin una previa preparación para actuar de forma responsable en él. Consecuentemente, la labor formativa y de sensibilización requeridas deben guiarnos en un buen uso de las nuevas tecnologías.

2.1. Enfoque multidimensional: su vinculación a otros riesgos y amenazas

Como se indica en la ESN, *"los riesgos y amenazas actuales no son estancos y no se les puede dar respuestas aisladas".* En el presente apartado, sin ánimo de realizar una análisis exhaustivo de las interconexiones existentes entre los distintos riegos y amenazas que son objeto de atención en la ESN, se realizan unas someras reflexiones, a grandes rasgos, sobre la importancia de ofrecer una visión integral, tanto en relación con el abordaje de los riesgos y amenazas como con las posibles respuestas a los mismos. Así podemos comprobar cómo en la ESN se atiende tanto al ciberespacio como al espacio exterior como nuevos ámbitos susceptibles de confrontación, pudiendo hablar de un nuevo campo de batalla, en el que pueden desarrollarse operaciones cibernéticas combinadas con operaciones bélicas convencionales o librarse íntegramente a través de operaciones cibernéticas, en lo que se ha llegado a denominar ciberguerra.

Por otra parte, la utilización del medio cibernético para la comisión de actos terroristas, lleva a atender una nueva modalidad de terrorismo: el ciberterrorismo. Las organizaciones terroristas se sirven de las nuevas tecnologías de la información y la comunicación para lograr sus objetivos. La facilidad con la que pueden acceder a este medio, con un bajo coste económico y aprovechando el anonimato en un contexto de sociedad global, hace de internet un medio idóneo para el reclutamiento de miembros, la obtención de recursos, la planificación y ejecución de atentados, así como agravar el impacto de sus acciones criminales. Las organizaciones del crimen organizado también se benefician de las características del ciberespacio para la comisión de sus acciones delictivas y criminales.

Como señala GONZÁLEZ CUSSAC, "la criminalidad organizada en general y el terrorismo en particular están generalizando el uso de las nuevas tecnologías de la información y la comunicación como instrumentos para desarrollar su actuación delictiva"[20]. A pesar de que, como acertadamente indica este autor, los cibercrímenes y las ciberamenazas no pueden ser consideradas categorías equivalentes, "determinadas formas de cibercriminalidad representan verdaderas amenazas a la seguridad nacional"[21], como son el terrorismo y la criminalidad organizada.

Atendiendo, además, la cada vez mayor conexión existente entre distintas organizaciones criminales entre sí y con grupos terroristas, se incorpora un plus de peligrosidad a las actividades de crimen organizado que, de por sí, ya son generadoras de otros riesgos y amenazas para la seguridad nacional, como el blanqueo de capitales. Vinculado al blanqueo de capitales, la ESN hace referencia expresa a los llamados paraísos fiscales, considerados como un factor desestabilizador del sistema. La inestabilidad económica y financiera, al igual que sucede con las ciberamenzas, es considerada como uno de los principales riesgos y amenazas para la seguridad nacional interna e internacional, por sí misma y por su conexión a otros riesgos existentes. Los ataques cibernéticos dirigidos a desestabilizar el sistema económico y financiero tienen graves consecuencias para toda la sociedad, pues las características propias del ciberespacio pueden acelerar y agravar dicho sistema, provocando *"el colapso económico y financiero tanto del sector público como del privado"*.

La seguridad energética se presenta como otro de los objetivos de la ESN. Por ello se debe garantizar un entorno seguro frente a posibles ciberataques a las infraestructuras críticas, entre las que se encuentran las infraestructuras energéticas. Como se recuerda, *"la energía es un factor clave para el progreso económico y el correcto funcionamiento de la sociedad"*.

Por otra parte, la proliferación de armas de destrucción masiva (tanto nucleares como químicas o biológicas), así como sus sistemas de lanzamiento representan una amenaza a la paz y la seguridad internacionales que tampoco queda ajena a la posibilidad de sufrir ciberataques, lo que multiplica exponencialmente la nocividad de sus efectos. En relación con las armas químicas y biológicas, uno de los grandes retos se centra en los sistemas de verificación y control de las exportaciones. Si además atendemos a que el mayor tráfico ilícito de armamento (tanto convencional como el que nos ocupa) se realiza a través del medio marino, resulta de gran importancia atender a otro riesgo y amenaza recogida en la ESN: la vulnerabilidad del espacio marítimo frente a los ciberataques, lo que exige una conciencia de ciberseguridad marítima, para lo que ha sido adoptada una

[20] GONZÁLEZ CUSSAC, J.L., Estrategias legales..., *op. cit.* en cita 9, p. 89.

[21] *Ibidem*, p. 120.

Estrategia de Seguridad Marítima Nacional[22] (en adelante, ESMN), en la que se establece que la proliferación de armas de destrucción masiva,

> *"tiene en el medio marino un elemento facilitador debido a las características inherentes de este espacio, en particular la dificultad de control, la continuidad y la discreción que ofrece, unido a una compleja aplicación del régimen jurídico"*.

Si las armas de destrucción masiva caen en poder de grupos terroristas, sus efectos nocivos se ven agravados, pudiendo afectar su utilización a los ciudadanos y a las estructuras críticas vitales de los Estados que han sido elegidos como objetivo de sus acciones criminales.

En cuanto a la interconexión entre la vulnerabilidad del espacio marino y las ciberamenazas, la ESMN dispone que:

> *"Al igual que sucede en otros sectores, el uso de las TIC en el ámbito marítimo incrementan la probabilidad de que se realicen ciberataques contra elementos esenciales para el desenvolvimiento de las actividades propias de este medio. Ello hace necesario proteger los sistemas de vigilancia y control, las infraestructuras marítimas críticas y los sistemas de navegación y comunicación"*.

Los flujos migratorios irregulares son objeto de atención y preocupación en la ESN, tanto en relación con la situación del Estado de origen que ha provocado dicha inmigración como su afectación a la cohesión social o a su proceso de integración social. En ambas vertientes, el uso nocivo de las nuevas tecnologías, especialmente en el ámbito de la comunicación e información, juegan un importante papel en la desestabilización de los Estados de origen y destino[23]. Por otra

[22] La Estrategia de Seguridad Marítima Nacional fue aprobada por el Consejo de Seguridad Nacional el 5 de diciembre de 2013. En ella se atienden a dos grandes grupos de riesgos y amenazas para la seguridad marítima nacional: 1) los derivados de actos deliberados y de naturaleza delictiva, entre los que se incluyen a las ciberamenazas; y 2) los de naturaleza accidental o fortuita que *"resultan consustanciales al mero contacto del hombre con la mar"*. Disponible en el sitio web: http://www.emad.mde.es/DOCUMENTOS-INTERES/documentos/documentosEMAD/140201-CIBERSEGURIDAD-SEGURIDAD-MARITIMA-RED.html

[23] Si uno de los grandes retos de la democracia consiste en la construcción de sociedades inclusivas de todos los sectores de la población, deben ponerse todos los medios legales y recursos del Estado a disposición de la erradicación de todas las acciones dirigidas a la erradicación de cualquier tipo de discriminación que impidan o dificulten la plena integración de los inmigrantes, tanto legales como ilegales. Las informaciones de corte discriminatorio difundidas a través del ciberespacio constituyen, además de una actividad delictiva, una amenaza a la cohesión social y un grave obstáculo que superar para la integración de los inmigrantes en la sociedad. La gravedad de esta amenaza adquiere un plus de gravedad si a través de ciberespacio se impulsa la comisión de los denominados *"hate crimes"* o crímenes de odio. Véase: *Estrategia integral contra el racismo, la discriminación racial, la xenofobia y otras formas conexas de intolerancia*, Ministerio de Trabajo e Inmigración, 2011; así como un documento de orden práctico, en el que se apuesta por la necesaria colaboración ciudadana y se atiende a los *"hate crimes"*: *Manual de apoyo para la formación de Fuerzas y Cuerpos de Seguridad en la identificación y registro de incidentes racistas o xenófobos*, Ministerio de Empleo y Seguridad Social, 2012.

parte, los flujos migratorios masivos suelen responder a procesos en los que se ven interconectados algunos de los riegos y amenazas ya enunciados (especialmente como consecuencia de su condición de víctima de los conflictos armados o víctima de actividades ilícitas desarrolladas por organizaciones de crimen organizado). A ello se puede unir otro riesgo o amenaza recogida en la ESN: las emergencias y catástrofes, que si bien pueden ser consecuencia de catástrofes naturales o bien de acciones humanas que, de forma accidental o intencionada, provocan una desestabilización del Estado con importantes efectos nocivos de la población y provocar, como consecuencia, flujos masivo de inmigración. En relación con las acciones humanas intencionadas, podíamos incluir los ciberataques a las infraestructuras críticas, aunque no se haga una referencia expresa a esta causa en la ESN.

La vulnerabilidad de las infraestructuras críticas son atendidas como una amenaza en sí misma considerada. Los riesgos y amenazas que acechan a las infraestructuras críticas no sólo afectan a la seguridad de la población, a su bienestar social y económico, a su salud y al mantenimiento de las funciones sociales básicas, sino también al correcto funcionamiento de las instituciones del Estado y de las Administraciones Públicas. Si estos riegos y amenazas tiene su origen en un ataque cibernético, una de las modalidades que la ESN califica de "mayor peligrosidad", los efectos dañinos para los ciudadanos y el propio Estado pueden llegar a ser devastadores.

Por último, no debemos dejar de dar unas pequeñas pinceladas a otro riesgo y amenaza cada vez más interconectado con las ciberamenzas: el espionaje. Si bien, como se recuerda en la ESN, *"las agresiones por parte de los Estados, grupos o individuos con la finalidad de lograr información que les permita obtener ventajas estratégicas, políticas o económicas, han sido una constante histórica y siguen siendo una amenaza de primer orden para la seguridad"*, su desarrollo a través del uso nocivo de las nuevas tecnologías ha desarrollado la modalidad del ciberespionaje, con una tendencia creciente de afectación en el ámbito del espionaje económico.

Los ciberataques, en cualquiera de sus modalidades, bien en el desarrollo de una operación cibernética durante un conflicto bélico, bien mediante una acción de ciberterrorismo, de cibercrimen o de *hacktivismo* producen efectos dañinos tanto a los ciudadanos como a las instituciones públicas y privadas. Las ciberamenzas, tanto consideradas como riesgo y amenaza con entidad propia como instrumento facilitador de otros riesgos y amenazas, ofreciendo un impacto dañino potencialmente superior en relación con su comisión por medios convencionales, hace necesaria una vital labor de formación y concienciación hacia los riesgos y amenazas cibernéticos con un enfoque integral. Esta labor formativa y de sensibilización dirigida a todos los sectores de la población se hace necesaria para poder responder de forma eficaz frente a las ciberamenazas, construyendo una conciencia de ciberseguridad basada en el conocimiento previo para el uso responsable de las nuevas tecnologías. En palabras de HIDALGO TARRERO, "El

tener consciencia de las ciberamenazas no quiere decir que haya que evitar hacer uso del ciberespacio, sino que significa hacer un uso responsable del mismo"[24].

Para poder atender a las previsiones establecidas en la ESN en el ámbito de protección del ciberespacio, se ha adoptado la Estrategia de Ciberseguridad Nacional[25] (en adelante, ECN), *"con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenzas"*. Por ello, a la hora de abordar una cultura de ciberseguridad se hace necesario atender de forma combinada la ESN y la ECN.

2.2. Apuesta por el multilateralismo como respuesta eficaz frente a una amenaza global

La ESN presenta retos y amenazas globales a las que se ha de responder con soluciones globales adoptadas por la comunidad internacional, siendo la cooperación y la acción multilateral su principio rector. Las ciberamenazas se erigen en el ejemplo de máxima globalidad al desarrollarse en un espacio global y transfronterizo, el ciberespacio. Si, como acertada y genéricamente (aplicable a todo tipo de riesgo y amenaza) se indica en la ESN, *"las respuestas unilaterales y aisladas no son eficaces, por su carácter incompleto y parcial, frente a unos retos que exigen un enfoque multidisciplinar y una acción conjunta"*, las ciberamenazas no pueden encontrar una respuesta eficaz más que a través de la cooperación interna entre todos los sectores de la sociedad y la acción multilateral internacional.

Además de los ámbitos organizativos ya atendidos, con un liderazgo a nivel universal de las Naciones Unidas y un compromiso claro hacia el multilateralismo de la UE, se hace necesario mencionar el ámbito de la OTAN, por el especial protagonismo que ha ido asumiendo en materia de ciberseguridad frente a las ciberamenazas, desde que se produjeran los ataques cibernéticos dirigidos a Estonia, en 2007, adoptando un novedoso Plan Estratégico y aportando un manual sobre ciberseguridad, conocido como Manual de Tallin[26]. No obstante, no hay

[24] HIDALGO TARRERO, J.T., "Principios de una conciencia nacional de ciberseguridad", en AA.VV, *Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario*, núm. 137 de la colección Monografías de la Escuela de Altos Estudios de la Defensa, Ministerio de Defensa, Madrid, 2013, p. 43.

[25] La Estrategia de Ciberseguridad Nacional fue aprobada por el Consejo de Seguridad Nacional, junto a la ESMN, el 5 de diciembre de 2013, pudiendo ser consultada en el siguiente sitio web: http://www.lamoncloa.gob.es/NR/rdonlyres/2A778417-DABC-4D36-89A2-3B81565C3B82/0/20131332EstrategiadeCiberseguridadx.pdf

[26] Si bien han sido muchos los autores que ya han atendido al liderazgo de la OTAN en materia de ciberseguridad, pueden destacarse las siguientes contribuciones: GANUZA ARTILES, H., "La situación de la Ciberseguridad en el ámbito internacional y de la OTAN", en *Cuadernos de Estrategia*, nº 149 , (Ejemplar dedicado a: *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio)*, IEEE-IUGM, Ministerio de Defensa, 2010, pp. 128-164. VELÁZQUEZ ORTIZ, A.P, "El Manual de Tallin: estudio y crítica de los principales conceptos y normas", en ALDA MEJÍAS, S. Y ÁNGEL SANTANO, S (Dir.), *La seguridad. Un concepto amplio y dinámico: V Jornadas de estudios de seguridad, Madrid, 7,8 y 9 de mayo de 2013*. Edit. IUGM, Madrid, 2013, pp. 607-633.

que olvidar las distintas interconexiones con otras amenazas, en cuya respuesta están asumiendo también un liderazgo otras organizaciones de ámbito regional europeo, como es el Consejo de Europa, en relación con el cibercrimen[27], o la OSCE, en relación con el ciberterrorismo, aunque a partir del año 2010 impulsó una nueva visión integral de la ciberseguridad.

En la ECN se establece el propósito de fijar directrices del uso seguro del ciberespacio, *"dentro del máximo respeto a los principios recogidos en la Constitución; en las disposiciones de la Carta de las Naciones Unidas, relativas al mantenimiento de la paz y seguridad internacionales, en coherencia con la Estrategia de Seguridad Nacional y con iniciativas desarrolladas en el marco europeo, internacional y regional"*. Se apuesta por el multilateralismo para la consecución de un ciberespacio seguro y fiable, así como para el establecimiento de estándares internacionales de ciberseguridad. En concreto, se promoverá el desarrollo de una política de ciberseguridad coordinada en la UE y en otras organizaciones internacionales de Seguridad y Defensa, al tiempo que reforzará sus relaciones de cooperación con la Agencia Europea de Defensa; la Agencia Europea de Seguridad de las redes y de la información; el Centro Europeo de Ciberdelincuencia; la OSCE; la OTAN; la OCDE; y, por supuesto, con las Naciones Unidas.

2.3. Claves para un adiestramiento/capacitación eficaz en materia de ciberseguridad

Los principios informadores de la ESN que marcarán las directrices de la Seguridad Nacional, pueden ser atendidos para abordar las claves de un adiestramiento/capacitación eficaz en materia de seguridad: Unidad de acción; anticipación y prevención; eficiencia y sostenibilidad de los recursos , así como resilencia.

La unidad de acción requiere la implicación, coordinación y armonización de todos los actores y recursos, buscando una mayor eficiencia y sostenibilidad de los mismos. La unidad de acción en cuanto a la implicación de todos los sectores de la sociedad en un "proyecto compartido" frente a las ciberamenazas se encuentra dirigida a ofrecer respuestas eficaces, no sólo desde el ámbito de la defensa militar, en las esferas de la prevención y la resilencia.

La anticipación y prevención resulta especialmente necesaria en relación con la cultura de ciberseguridad, pues se requiere que todos los actores implicados

[27] En el seno del Consejo de Europa se adoptó, el 23 de noviembre de 2001, la *Convención contra la Ciberdelincuencia*, tendente a la necesaria tipificación en los respectivos ordenamientos penales de los distintos delitos informáticos (desde los delitos de falsificación y fraude informáticos, pasando por los evidentes delitos contra la confidencialidad, integridad y disponibilidad de ordenadores, datos y sistemas, hasta los delitos contra la propiedad intelectual y contra la intimidad. En esta Convención también se realiza una apuesta al multilateralismo para ofrecer respuestas eficaces frente a los ciberdelitos. España ratificó la Convención en 2010 (BOE núm. 226, de 17 de noviembre de 2010).

cooperen en la detección y la reconducción de situaciones que puedan poner en peligro la Seguridad Nacional.

La resilencia, concebida en la ESN como *"la aptitud de los recursos humanos y materiales para afrontar con flexibilidad y fortaleza las situaciones de crisis y sobreponerse a ellas minimizando y absorbiendo sus competencias negativas"* , conforma otro de los elementos estratégicos de gran importancia para la consolidación de una cultura de ciberseguridad.

Un último comentario en relación a los principios informadores de la ESN, lo dedicamos a la eficiencia y sostenibilidad de los recursos. Resulta cuanto menos paradójico el hecho de que nos enfrentamos ante una amenaza de bajo coste, de fácil utilización y accesibilidad y que, por el contrario, requiere una importante reasignación de recursos humanos y económicos para su erradicación o, al menos, para la mitigación de sus efectos nocivos. Gran parte de esos esfuerzos humanos y económicos han de dirigirse a ofrecer una formación de toda la población, graduada en distintos niveles acordes con los usos tecnológicos (por edad y sectores de la población, incluyendo los usos de las nuevas tecnologías en los hogares, colegios, etc) y una capacitación especializada a determinados sectores de la población (Administraciones pública y autonómicas; empresas públicas, privadas o autónomas; militares; etc). Otra gran parte, debería destinarse a proyectos de I+D+I especialmente destinados al ámbito de la ciberseguridad, en busca de un ciberespacio cada vez más seguro.

La ECN, en sintonía con los principios rectores de la ESN, asumidos con una extensión de los mismos, recoge los siguientes principios rectores: liderazgo nacional y coordinación de esfuerzos; responsabilidad compartida; proporcionalidad, racionalidad y eficacia; y, por último, cooperación internacional;

> *"Y todos ellos, respetando y fortaleciendo la protección y el pleno disfrute de los derechos fundamentales consagrados en nuestra Constitución y en instrumentos internacionales de la importancia de la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos o el Convenio Europeo para la protección de los Derechos Humanos y la Libertades Fundamentales. El Gobierno de España se compromete a desarrollar políticas que, mejorando la seguridad de los Sistemas de Información y de Telecomunicaciones que emplean los ciudadanos, profesionales y empresas, preserven los derechos fundamentales de todos ellos, especialmente en los sectores más desprotegidos"*.

En consecuencia, las respuestas que se ofrecen desde la ESN y la ECN a las distintas modalidades de ataques cibernéticos han de encontrarse bajo el paraguas de los principios, valores y derechos constitucionales.

3. BREVES REFLEXIONES SOBRE LA NECESARIA CAPACITACIÓN ESPECIALIZADA EN Y DESDE LA UNIVERSIDAD

Atendiendo al Informe de 2012 del Spanish Cyber Security Institute (en adelante, SCSI) ,

> "el objetivo principal de la Ciberseguridad Nacional es proporcionar un ciberespacio seguro que garantice la prosperidad social, cultural y económica de nuestro país así como las libertades fundamentales de los ciudadanos a través de una cultura basada en la prevención y resilencia en la que participen, de manera activa e integrada, todos los sectores de la sociedad"[28].

Para su consecución, el Informe del SCSI incluye tres objetivos parciales a alcanzar: un conocimiento de ciber-situación fiable y actualizado; mejorar la resilencia nacional frente a la amenaza cibernética; y crear y fomentar una cultura de ciberseguridad. En relación con este tercer objetivo destaca la necesidad de establecer un programa nacional de educación en materia de ciberseguridad, sugiriendo las siguientes acciones: desarrollo de un campaña nacional de ciberconcienciación; inclusión en los planes de estudio de todos los niveles educativos (desde la primaria hasta la post-universitaria) de materias relacionadas con uso responsable de las nuevas tecnologías y específicas en relación con la ciberseguridad; modificación de los programas educativos en las materias relacionadas con Ciencia, Tecnología e Ingeniería, sin olvidar los aspectos legislativos y normativos; incorporación de materias relacionadas con las nuevas tecnologías y la ciberseguridad tanto en los planes de estudio de las academias militares como en las escuelas de negocios; creación de un programa de centros de excelencia en materia de ciberseguridad; planes de formación y concienciación, de carácter obligatorio, destinado a empleados de empresa pública, privada y autónoma.

La ECN viene a dar respuesta a las propuestas del SCSI, a través de sus líneas de acción, entre las que podemos destacar algunas de ellas: desarrollar un marco de conocimientos de ciberseguridad en los ámbitos técnico, operativo y jurídico; extender y ampliar programas de captación de talento, investigación avanzada en ciberseguridad en cooperación con Universidades y centros especializados (ambas acciones enunciadas en la Línea de acción 6). La línea de acción 7, bajo el título de "Cultura de Ciberdefensa" incluye las siguientes acciones: impulsar actividades de sensibilización dirigidas a los ciudadanos y empresas sobre cómo proteger mejor su entorno tecnológico; desarrollar programas de Concienciación

[28] AA.VV, *La Ciberseguridad Nacional un compromiso de todos. La necesidad de evolucionar de una cultura reactiva a una de prevención y resilencia*, Spanish Ciber Security Institute, junio 2012. Disponible en la página web: https: //www.inteco.es.

en Ciberseguridad, en colaboración con agentes del sector público y privado; fomentar mecanismos de apoyo a las empresas y profesionales en el uso seguro de las TIC; y, por último, *"asesorar y dar soporte al desarrollo de módulos educativos de sensibilización en ciberseguridad, dirigidos a todos los niveles de la enseñanza"*.

Además, en relación con otros sectores específicos de la sociedad, la ECN también atiende a la necesaria capacitación especializada que deben recibir para el desarrollo de sus funciones. De este modo, en la Línea de acción 1 se establece la necesidad de

> *"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"*.

De igual manera se incluye la necesaria capacitación especializada dirigida a los profesionales del ámbito jurídico, en relación con el cibercrimen y la ciberdelincuencia, en la Línea de acción 4:

> *"Asegurar a los profesionales del Derecho el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimientos en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado. En este sentido, es especialmente importante la cooperación con el Consejo General del Poder Judicial, la Abogacía del Estado, la Fiscalía General del Estado, la Fiscalía Coordinadora de la Criminalidad Informática y el Consejo General de la Abogacía Española"*.

Es evidente que las Universidades están llamadas a asumir un protagonismo destacado para el establecimiento de una paulatina cultura de ciberseguridad en sus propias instituciones y desde ellas al resto de la sociedad en su conjunto, con especial incidencia en aquellos sectores especialmente implicados: profesionales del Derecho, militares y empresarios.

3.1. Capacitación especializada en el ámbito universitario

Si como decía ORTEGA Y GASSET[29], "la raíz de la reforma universitaria está en acertar plenamente con su misión", debemos aprovechar el nuevo gran proceso de reforma en la que se encuentra inmerso el ámbito universitario. El nuevo Espacio Europeo de Educación Superior (en adelante, EEES) ofrece una oportunidad para reflexionar y repensar la misión de la Universidad, tanto en

[29] ORTEGA Y GASSET, J., *Misión de la Universidad y otros Ensayos afines*, Ediciones de la Revista de Occidente, 6ª Ed., Madrid, 1976, p. 29.

relación con la formación integral del alumno durante su vida universitaria como en relación con el servicio que se ofrece a la sociedad al dotarles de profesionales cualificados para ejercer sus funciones en un nuevo contexto globalizado y en constante evolución.

La formación integral del alumno debe atender a una formación y capacitación de excelencia a través del dominio de las distintas competencias y habilidades profesionales adquiridas a través de los correspondientes planes de estudio, pero además, deben ser formados para ser agentes de cambio de la sociedad, deben ser agentes responsables y comprometidos en el mantenimiento y reforzamiento del estado social y democrático conseguido. En este sentido, el EEES invita a una continua reflexión sobre los planes de estudio y, en definitiva, sobre el perfil de los futuros profesionales que deben salir de la Universidad. Una sociedad democrática avanzada requiere excelentes profesionales comprometidos con los principios y valores constitucionales, entre los que se encuentra la seguridad. Apostar por la consolidación de una cultura de ciberseguridad cimentada en una sólida cultura de seguridad y defensa implica apostar por la paz.

Además, la Universidad no debe dejar de dirigir su mirada hacia las necesidades de la sociedad a la que ofrecerá verdaderos agentes de cambio. El reto, pues, de implicar a las instituciones universitarias en un proceso paulatino de instauración en la sociedad de una cultura de ciberseguridad, cimentada en una sólida cultura de seguridad y defensa, debe obtener su respuesta dentro del ámbito universitario y desde él hacia la sociedad en general y hacia determinados sectores de la población en particular.

Si las sociedades democráticas más avanzadas han sabido consolidar una cultura de seguridad y defensa respetuosa con el imperio de la ley y el respeto de los Derechos Humanos, la Universidad está llamada a ser un motor impulsor del establecimiento de una cultura de seguridad y defensa como instrumento clave para la consecución de una cultura de ciberseguridad en el contexto de un Estado social y democrático de Derecho. Por ello, se hace necesaria una labor de sensibilización y formativa dirigida a la consecución de una cultura de ciberseguridad, a partir del fortalecimiento de una conciencia nacional, mediante el desarrollo de competencias genéricas y específicas que permitan la transmisión de los principios y valores democráticos. Por otra parte, a través de competencias específicas de carácter conceptual que permitan, desde un enfoque teórico-práctico, atender a las peculiaridades de la amenazas cibernéticas, desde un enfoque multidimensional y transversal.

3.2. Hacia una cultura de ciberseguridad en y desde la Universidad

Para la consecución del arraigo de una cultura de ciberseguridad en la sociedad española, se requiere desplegar esfuerzos en el ámbito de la sensibilización

y la capacitación adecuada que permita una participación activa de todos en un "proyecto compartido" frente a la amenaza cibernética. En relación con las actuaciones de sensibilización y capacitación especializada, las instituciones universitarias españolas están llamadas a asumir un protagonismo destacado. Sin embargo, no podrá cumplir de forma eficiente su función, si, con carácter previo, no se consigue instaurar una cultura de ciberseguridad, cimentada en una cultura de seguridad y defensa, dentro del propio ámbito universitario. Consecuentemente, resulta necesario, la implicación de todos sus actores: personal docente e investigador (en adelante, PDI); personal de administración y servicios (en adelante, PAS) y alumnos. A todos ellos debe ir dirigida una labor formativa y de sensibilización no sólo dirigida al uso responsable de las TIC, sino a crear una conciencia universitaria de ciberseguridad, en la que los diferentes usuarios de las TIC sean conscientes de que su actuación está contribuyendo a la defensa nacional interna e internacional.

En la gran reforma en la que se encuentra inmersa la universidad española se ha tener en consideración, a la hora de reasignar sus recursos humanos y económicos, la necesidad de ofrecer un entorno cibernético seguro para el desarrollo de todas las actividades universitarias y la contribución a la creación de una conciencia cibernética que redunde en el arraigo de una cultura de ciberseguridad en la Universidad y desde ella a toda la sociedad. Por ello, se requiere, por una parte, reforzar las funciones a desempañar por los responsables de seguridad de las unidades o servicios TIC de los centros universitarios. El reforzamiento de los servicios de seguridad TIC resulta imprescindible para el desarrollo de una actividad universitaria en un entorno cibernético seguro. Por otra, el crear un entorno cibernético seguro dentro de un plan de formación integral de todos los actores del ámbito universitario, a través de en un plan programado de formación continua, tendente a la consolidación de una cultura de ciberseguridad en la Universidad.

Las instituciones universitarias no han sido ajenas a las oportunidades que les brindaban las nuevas TIC, que han ido incorporando en su actividad diaria: desde la matriculación on-line; servicios de préstamos bibliotecarios; los campus virtuales de enseñanza; y así hasta una infinidad de actividades que son desarrolladas en el ciberespacio, sin ser conscientes de los riesgos y amenazas para la Seguridad nacional y el pleno disfrute de los derechos Humanos y libertades fundamentales, si no se hace un uso responsable del mismo.

Además del necesario reforzamiento de las capacidades de los servicios de seguridad TIC. La consecución de una cultura de ciberseguridad en el ámbito universitario requiere una implicación activa del PDI, fundamentalmente a través de actividades que le son propias: docencia curricular, tanto en los niveles de grado y postgrado; de investigación y de organización de actividades de extensión universitaria, sobre los que realizaremos unos pequeños apuntes.

3.2.1. Docencia

Como se ha indicado, la ECN incluye en su Línea de acción 7 el propósito de apoyar el desarrollo de módulos educativos de concienciación en materia de ciberseguridad en todos los niveles educativos, incluyendo el universitario. Consecuentemente, han de ser atendidos en todas las Universidades y en todas sus Escuelas y Facultades. Como se ha indicado, la labor formativa y sensibilizadora de toda la comunidad universitaria dirigida a la consecución de un entorno cibernético seguro y una cultura de ciberseguridad requiere, por una parte, el establecimiento de módulos específicos (por ejemplo, a través de módulos dentro de programas de diplomas adjuntos al título; o dentro de los programas de formación continua del PDI y del PAS). Pero además, si tenemos en consideración que, como hemos venido defendiendo, una cultura de ciberseguridad sólo puede ser eficaz si se incluye dentro de una cultura de seguridad y defensa, se hace necesario que se revisen los planes de estudio de grado y de postgrado; o que al menos, se revisen las guías docentes de los diferentes planes de estudios, para reflexionar si el perfil de los futuros profesionales que saldrán de nuestras aulas aportará a la sociedad verdaderos agentes de cambios comprometidos a defender los principios y valores democráticos.

Sin embargo, la necesidad de ofrecer una capacitación más especializada frente a las amenazas cibernéticas tiene que ir dirigida a dos campos del saber muy concretos: los vinculados con la Ciencia y la Tecnología y el Jurídico. En este sentido, si atendemos al liderazgo que ha de asumir una institución universitaria, se requiere la inclusión de asignaturas curriculares, tanto de grado como de postgrado, en sintonía con las propuestas incluidas en el Informe del SCSI.

No debemos olvidar tampoco que, tanto en la ECN como en el referido Informe del SCSI, que existen determinados sectores de la población que deben recibir una especial capacitación, a saber: el personal militar y de inteligencia; los empresarios y los profesionales del Derecho. Se requiere reforzar el papel de la Universidad en los procesos de formación continua de profesionales, tanto en relación con el establecimiento de un espacio cibernético seguro como con el arraigo de una cultura de seguridad y defensa.

Estos cambios, que a modo de ejemplo, son atendidos en el ámbito de la docencia, no serán posibles si no existe una concienciación en la materia por parte de los responsables políticos, con el desarrollo de las oportunas políticas públicas en el ámbito de la enseñanza universitaria; de las Administraciones públicas y autonómicas; y de los organismos de los que depende la acreditación de los distintos planes de estudio, como es el caso de la Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA).

3.2.2. Investigación

Hasta el momento, los estudios e investigaciones sobre cuestiones relativas a la seguridad y la defensa ha quedado reducido a acciones individuales de profesores universitarios que yendo "contracorriente" y con grandes esfuerzos - no han sido consideradas hasta la actualidad (y aún hoy tímidamente) como líneas prioritarias a la hora de acceder a recursos económicos públicos y/o privados para financiar sus investigaciones- han ido incorporando en sus respectivas Universidades una sensibilización hacia la materia que nos ocupa. Los únicos grandes apoyos a la investigación universitaria en cuestiones de seguridad y defensa han venido precisamente de la mano del Ministerio de Defensa, impulsando desde hace más de una década la implicación del mundo universitario. El panorama de futuro se muestra algo alentador, gracias al impulso dado por la Unión Europea a través del marco del programa Horizonte 2020, aunque en su implementación en España ha quedado reducido al ámbito científico y tecnológico. Se requiere reforzar las acciones de I+D+I en el ámbito de la ciencia jurídica en relación con una materia tan sensible, como es la ciberseguridad, ya que las respuestas frente a las ciberamenazas deben ajustarse a la legalidad interna e internacional. La necesidad de adecuar y reforzar el marco legislativo interno e internacional se presenta como un importante reto en el ámbito jurídico universitario, por lo que debe existir una mayor implicación del sector público y privado, ofreciendo el apoyo necesario para abordar investigaciones sólidas en la materia.

Estas circunstancias nos impide colocarnos a la altura de las investigaciones que se desarrollan en los Estados con democracias avanzadas. LÓPEZ MORA señala cómo,

> "[...] los estudios sobre seguridad y defensa conforman un dominio universitario arraigado de alcance internacional y, muy especialmente, su presencia sobresale en los contextos académicos europeos y norteamericanos. Todo lo anterior se manifiesta desde hace al menos media centuria de trabajos consistentes y dedicación experta"[30]

Para arraigar una cultura de ciberseguridad cimentada en una sólida cultura de seguridad y defensa hace falta no sólo voluntad política, sino una importante reasignación presupuestaria destinada a proyectos de I+D+I, preferentemente en los campos científicos-tecnológicos y jurídicos. La difusión de los resultados de las investigaciones resultan un elemento clave para la contribución de una cultura de ciberseguridad adecuada a las necesidades de una sociedad democrática avanzada.

[30] LÓPEZ MORA, F., "La cultura de la seguridad y defensa en el ámbito universitario", en *Cuadernos de Estrategia* núm. 155, (Ejemplar dedicado a: *La Cultura de seguridad y defensa. Un proyecto en marcha)*, IEEE, Ministerio de Defensa, Madrid, 2011, p. 95.

Por otra parte, se requiere intensificar la creación de equipos de investigación de composición mixta, civil (procedentes del ámbito académico y de los sectores especialmente implicados) y militar, e interdisciplinar, en consonancia con el enfoque integral de la Seguridad nacional interna e internacional dirigida a un "un proyecto compartido", tal y como se establece en la ESN. Sin embargo, no se producirán avances si dentro de las propias instituciones universitarias no se arraiga una cultura de ciberseguridad cimentada en una sólida cultura de seguridad y defensa.

3.2.3. Actividades de extensión universitaria

Las actividades de extensión universitaria consistentes en la celebración de ciclos de conferencias, jornadas, congresos, seminarios, cursos de verano; etc., constituyen una gran oportunidad para contribuir a la labor formativa y de sensibilización en materia de ciberseguridad.

Podemos hablar de la existencia de un gran "cajón de sastre" del que se pueden extraer los materiales necesarios para realizar cualquier traje a medida, todo depende del resultado que se desee obtener. A modo de ejemplo, se pueden mencionar algunas de estas actividades de extensión universitaria, haciendo referencia a sus destinatarios y su contribución al establecimiento de una cultura de ciberseguridad cimentada en una sólida cultura de seguridad y defensa:

Las Jornadas y Congresos pueden ir dirigidos a un público experto o a un determinado sector de la sociedad y/o a la sociedad en general. Este tipo de actividad dirigida a un público experto se convierten en verdaderos foros de diálogo y en una oportunidad para unir sinergias y "hacer grupo", por lo que resulta necesario contar no sólo con expertos académicos, sino con otros sectores de la sociedad que desarrollan su actividad profesional vinculada a cuestiones relacionadas directa o indirectamente con la seguridad y la defensa, en sentido *lato*, y con la ciberseguridad, en particular. A pesar de estar dirigidas a un público experto, resulta interesante la asistencia de alumnos universitarios, especialmente de postgrado, con una finalidad formativa y de sensibilización, dirigida a impulsar futuros trabajos de investigación de fin de máster o de doctorado.

Este tipo de actividades también pueden ir dirigidas de forma principal a los alumnos pertenecientes a determinadas Escuelas o Facultades, cumpliendo también su función formativa y de sensibilización. A este tipo de actividad, resulta oportuno abrir su asistencia a la sociedad en general. Los ciclos de conferencias, también pueden cumplir esta función divulgativa, dirigiendo y, consecuentemente, modulando el mensaje apropiado al público receptor.

Los seminarios internos permiten reforzar la constitución de "grupos" dentro de la Universidad. La celebración de seminarios externos, permite unir sinergias en el ámbito de la investigación multidisciplinar e interfacultativa. Se requiere,

pues, un mayor apoyo por parte de las instituciones universitarias a la celebración de seminarios permanentes, tanto internos como externos, como un eficaz instrumento para la construcción de una masa crítica en materia de ciberseguridad y sobre cuestiones de seguridad y defensa en general.

Las denominadas actividades de extensión universitaria brindan un excelente foro de encuentro, de sensibilización y de debate, pero son insuficientes si no se aprovechan las sinergias creadas a través de actividades concretas de docencia y de investigación.

4. CONCLUSIONES

PRIMERA. Las estrategias de seguridad adoptadas por los Estados que gozan de una democracia avanzada constituyen un instrumento eficaz para la implantación de una cultura de ciberseguridad en sus respectivas sociedades, pero requieren de un eficaz desarrollo legislativo y un verdadero compromiso por parte del Gobierno y de las Administraciones y organismos públicos para que su arraigo sea una realidad y además, el adecuado. Como se ha indicado, tanto la ESN como la ECN –e incluso en la ESMN– muestran con claridad la dimensión global, multidimensional y relacional de las ciberamanezas. Sin embargo, aunque resultan ser unos instrumentos necesarios para la implantación de una cultura de ciberseguridad no son suficientes para su arraigo en la sociedad. Por otra parte, se hace necesario el cuestionarse si es posible el arraigo de una cultura de ciberseguridad en una sociedad en la que aún no exista una sólida cultura de seguridad y defensa. En este sentido, consideramos inviable la eficacia de una cultura de ciberseguridad que no se encuentre cimentada en una cultura de seguridad y defensa más amplia. En este sentido, los responsables de diseñar un plan de actuación -acción unitaria- frente a las ciberamenazas, no deberían olvidar la necesidad de insertarlo dentro del marco de una cultura de la seguridad y la defensa nacional, interna e internacional. Consecuentemente, el arraigo de una cultura de ciberseguridad conlleva dos grandes retos: En primer lugar, arraigar una cultura de seguridad y defensa en la sociedad y desde ella, sin solución de continuidad, construir la bases para la consolidación de una cultura de ciberseguridad.

SEGUNDA.. La consolidación de una cultura de ciberseguridad requiere, al mismo tiempo, reforzar la consolidación de una cultura de seguridad y defensa que impulse una participación de todos los sectores de la sociedad a través de una ingente labor formativa y divulgativa para valorar lo que tenemos –principios, valores y derechos constitucionales– (conciencia nacional); conocer cuáles son los peligros que la acechan o puedan poner en peligro (conciencia de defensa) y estar dispuestos a defenderlos (cultura de seguridad y defensa). Junto a ello, se requiere el arraigo de una conciencia de ciberseguridad que nos permita responder

de forma eficaz, proporcional y legítima a la amenaza cibernética que puede poner en peligro los principios y valores democráticos o, incluso, la propia pervivencia del Estado.

TERCERA. El establecimiento de una cultura de ciberseguridad exige una labor de capacitación de todos los sectores de la sociedad, para la que está llamada a jugar un papel protagonista la Universidad. Atendiendo a que las ciberamenazas se desarrollan a través de un singular espacio, el ciberespacio, en el que todos los sectores de la población desarrollan sus actividades cotidianas de índole social, económica, profesional, etc., se requiere la implicación de toda la sociedad. Las instituciones universitarias no pueden quedarse ajenas y deben participar en el "proyecto compartido" que nos presenta la ESN, en un doble sentido: contribuyendo a crear un ciberespacio universitario seguro y liderando el arraigo de una cultura de ciberseguridad, cimentada en una cultura de seguridad y defensa, dentro de la Universidad y desde la Universidad a la sociedad. En este sentido, se ha de hacer una reflexión a fondo sobre la misión de la Universidad en un contexto democrático respetuoso con los principios y valores que cimientan nuestra Constitución, a través de actividades que le son propias: docencia, investigación y gestión. Las instituciones universitarias deben ofrecer a la sociedad profesionales cualificados y responsables con la defensa de un Estado social y democrático de Derecho.

Si bien el proceso de creación una cultura de ciberseguridad en España presenta grandes dificultades, atendiendo a que aún no está bien consolidada una conciencia de seguridad y defensa sobre la que cimentarse, resulta relevante el hecho de que el proceso ya se ha iniciado. Podemos afirmar que el proceso de instauración de una cultura de ciberseguridad, cimentada en una cultura de seguridad y defensa, en el ámbito universitario ya se ha puesto en marcha. Si bien es cierto que hasta el momento los esfuerzos realizados no responden al arraigo de una sólida cultura de seguridad y defensa en las instituciones universitarias, sino a iniciativas individuales, también lo es el que tampoco podemos negar que exista "grupo", en línea con el pensamiento de ORTEGA Y GASSET, quien, reflexionando sobre la reforma que en su día abordaba la Universidad, consideraba importante contar con esfuerzos individuales, aunque no diesen los frutos deseados si no existía grupo . Evidentemente, no podrá arraigarse en la Universidad una cultura de ciberseguridad, adecuadamente cimentada, si no existe grupo. Pero al igual que él y parafraseándole, podemos plantearnos el siguiente interrogante: "[...] Por qué dudar de que exista un grupo capaz de realizar esa reforma?"[31]. Sirvan estas reflexiones para interrogarnos sobre si en la Universidad seremos capaces de crear un grupo que contribuya a la consolidación de una cultura de ciberseguridad cimentada en una sólida

[31] ORTEGA Y GASSET, J., *Misión de la Universidad...*, *op. cit.* en cita 20 *supra*.

cultura de seguridad y defensa dentro de la Universidad y desde la Universidad contribuir a su consolidación en la sociedad.

BIBLIOGRAFÍA

AA.VV, *Manual de apoyo para la formación de Fuerzas y Cuerpos de Seguridad en la identificación y registro de incidentes racistas o xenófobos*, Ministerio de Empleo y Seguridad Social, 2012.

AA.VV, La Ciberseguridad Nacional un compromiso de todos. La necesidad de evolucionar de una cultura reactiva a una de prevención y resilencia. Spanish Ciber Security Institute, Junio 2012. Disponible en la página web: https: //www.inteco.es. (Fecha última consulta: Marzo 2014)

ARGUMOSA, J., "Una estrategia moderna de seguridad nacional", Revista *Política Exterior*, Vol. 24, núm. 138, noviembre-diciembre 2010, pp. 80-90.

AVILÉS FARRÉ, "Por un concepto amplio de seguridad", en AA.VV, *Revisión de la Defensa Nacional*. Número 55 de la colección Monografías del Centro Superior de Estudios de la Defensa Nacional, Madrid, 2002. pp.16-44.

BLANC ALTEMIR, A., "Introducción: Las Naciones Unidas y la Unión Europea: valores y ámbitos de acción compartidos en aras de una multilateralismo más eficaz", en BLANC ALTEMIR, A. (Dir.), *Las relaciones entre las Naciones Unidas y la Unión Europea. Seguridad, Cooperación y Derechos Humanos*, Edit. Tecnos, Madrid, 2013, pp. 17-65.

CONDE DE ARJONA, J., "La Cultura de Seguridad y Defensa en los países de nuestro entorno", *Cuadernos de Estrategia*, nº 155, (Ejemplar dedicado a: *La Cultura de Seguridad y Defensa. Un proyecto en marcha*), Ministerio de Defensa, Madrid, 2011; pp. 104-40.

GANUZA ARTILES, H., "La situación de la Ciberseguridad en el ámbito internacional y de la OTAN", *Cuadernos de Estrategia* nº 149, (Ejemplar dedicado a: *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio)*, IEEE-IUGM, Ministerio de Defensa, 2010, pp. 128-164.

GONZÁLEZ CUSSAC, J.L., "Estrategias legales frente a las ciberamenazas", *Cuadernos de Estrategia*, núm. 149, (Ejemplar dedicado a: Ciberseguridad. Retos y amenazas a la ciberseguridad en el ciberespacio), IEEE, Ministerio de Defensa, Madrid, 2011, pp. 83-127.

HIDALGO TARRERO, J.T., "Principios de una conciencia nacional de ciberseguridad", en AA.VV, *Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario*. Número 137 de la colección Monografías de la Escuela de Altos Estudios de la Defensa, Ministerio de Defensa, Madrid, 2013, pp. 35-70.

LABOIRE IGLESIAS, M., *La Estrategia de Seguridad Nacional (Mayo 2013)*, en Instituto Español de Estudios Estratégicos, Documento de Análisis núm. 34/2013, de 3 de junio de 2013, pp. 1-5. (Fecha última consulta: Abril 2014)

LÓPEZ MORA, F., "La cultura de la seguridad y defensa en el ámbito universitario", *Cuadernos de Estrategia* núm. 155, (Ejemplar dedicado a: *La Cultura de seguridad y defensa. Un proyecto en marcha*), IEEE, Ministerio de Defensa, Madrid, 2011, pp. 86-103.

ORTEGA Y GASSET, J., *Misión de la Universidad y otros Ensayos afines*, Ediciones de la Revista de Occidente, 6ª Ed., Madrid, 1976, p. 29.

SERRA RESACH, E., "Introducción", *Cuadernos de Estrategia* nº 155, (Ejemplar dedicado a: *La Cultura de Seguridad y Defensa. Un proyecto en marcha*), IEEE, Ministerio de Defensa, Madrid, 2011, pp. 11-26.

VELÁZQUEZ ORTIZ, A.P, "El Manual de Tallin: estudio y crítica de los principales conceptos y normas", en ALDA MEJÍAS, S. Y ÁNGEL SANTANO, S (Dir.), *La seguridad. Un concepto amplio y dinámico: V Jornadas de estudios de seguridad, Madrid, 7, 8 y 9 de mayo de 2013*; Edit. IUGM, Madrid, 2013, pp. 607-633.

Otra Documentación (nacional e internacional):

– *Estrategia Española de Seguridad. Una responsabilidad de todos*. Gobierno de España, 2011. Disponible en la siguiente página web : http://www.lamoncloa.gob.es/nr/rdonlyres/d0d9a8eb-17d0-45a5-adff-46a8af4c2931/0/estrategiaespanoladeseguridad.pdf (Fecha última consulta: Mayo 2014)

– *Estrategia integral contra el racismo, la discriminación racial, la xenofobia y otras formas conexas de intolerancia*, Edit. Ministerio de Trabajo e Inmigración, 2011.

– *Estrategia de Seguridad Nacional. Un proyecto compartido*. Presidencia del Gobierno, 2013. Disponible en la siguiente página web: http://www.lamoncloa.gob.es/nr/rdonlyres/d0d9a8eb-17d0-45a5-adff-46a8af4c2931/0/estrategiaespanoladeseguridad.pdf (Fecha última consulta: Mayo 2014)

– *Estrategia de Ciberseguridad Nacional*. Consejo de Seguridad Nacional. Presidencia del Gobierno, 2013. Disponible en el sitio web: http://www.lamoncloa.gob.es/NR/rdonlyres/2A778417-DABC-4D36-89A2-3B81565C3B82/0/20131332EstrategiadeCiberseguridadx.pdf (Fecha última consulta: Mayo 2014)

– *Estrategia de Seguridad Marítima Nacional*. Consejo de Seguridad Nacional. Presidencia del Gobierno, 2013. Disponible en el sitio web: http://www.emad.mde.es/DOCUMENTOS-INTERES/documentos/documentosEMAD/140201-CIBERSEGURIDAD-SEGURIDAD-MARITIMA-RED.html (Fecha última consulta: Mayo 2014).

– Carta de las Naciones Unidas.

– *Convención contra la Ciberdelincuencia*, adoptada por el Consejo de Europa el 23 de noviembre de 2001 (BOE núm. 226, de 17 de noviembre de 2010).

– *"Un programa de paz: diplomacia preventiva, establecimiento de la paz y mantenimiento de la paz"*, Informe del Secretario General, presentado de conformidad con la declaración aprobada el 31 de enero de 1992 en la Reunión en la Cumbre del Consejo de Seguridad, de 17 de junio de 1992. Doc: S/24111.

– *Declaración sobre el mejoramiento de la cooperación entre las Naciones Unidas y los acuerdos u organismos regionales en el mantenimiento de la paz y la seguridad internacionales*, Resolución 49/57 de la Asamblea General de las Naciones Unidas, adoptada el 9 de diciembre de 1994. Doc: A/RES/49/57.

– *Suplemento de "Un programa de paz"*, Documento de posición del Secretario General presentado con ocasión del cincuentenario de las Naciones Unidas, de 25 de enero de 1995. Doc: S/1995/1.

– *"Informe Brahimi" o Informe del Grupo sobre Operaciones de Mantenimiento de la Paz de las Naciones Unidas*. Doc: A/55/305-S/2000/809.

– "Declaración del Milenio" de la Asamblea General (Resolución 55/2 de la Asamblea General, adoptada el 13 de septiembre de 2000) Doc: A/RES/55/2.

– *Documento Final de la Cumbre Mundial 2005*. Doc: A/RES/60/1.

– *Resolución 1631*, adoptada por el Consejo de Seguridad en su 5282ª sesión, celebrada el 17de octubre de 2005- Doc. S/RES/1631 (2005).

– Resolución *"Promoción de un orden internacional democrático y equitativo"* aprobada por la Asamblea General el 18 de diciembre de 2013. Doc. A/RES/68/175.

– Resolución "Promoción de un orden internacional democrático y equitativo" aprobada por la Asamblea General el 18 de diciembre de 2013. Doc. A/RES/68/175.

– Informe del Grupo de alto nivel sobre las amenazas, los desafíos y el cambio: *"Un mundo más seguro: la responsabilidad que compartimos"*. Doc. A/59/565, de 2 de diciembre de 2004.