LA ESTRATEGIA DE SEGURIDAD NACIONAL. CIBERDEFENSA Y SEGURIDADES MARÍTIMA Y ENERGÉTICA

Antonio MORENO-TORRES GÁLVEZ
Ingeniero industrial del Estado

(RV)

Introducción

A revisión de 2013 de la Estrategia de Seguridad Nacional (ESN) identifica una serie de ámbitos de actuación que requieren, cada uno de ellos y por separado, de una profundización específica en atención a sus peculiaridades en términos de riesgos y amenazas. Hasta la fecha, tres han sido los desarrollados: ciberseguridad (en 2013), seguridad marítima (en 2013) y seguridad energética (este último, muy recientemente, en julio de 2015).

En este artículo se hará una breve revisión del paraguas que supone la ESN, analizando cómo se cobijan bajo el mismo las actuaciones en los tres ámbitos citados, y haciendo hincapié en cómo todas las perspectivas de la Seguridad Nacional están interrelacionadas, lo que justifica el enfoque global de la cuestión.

La Estrategia de Seguridad Nacional

El punto de partida de la ESN es la caracterización de la Seguridad Nacional como un servicio público, de carácter integral y amplio, definido como «la 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». Con esta naturaleza de política de Estado en mente, y desde el reconocimiento de la dimensión *global* de la seguridad, que al verse afectada por retos planetarios requiere una cooperación internacional que coexista con el necesario requisito de *autonomía*, se identifican los siguientes elementos básicos en la ESN:

- Cuatro *principios informadores*: unidad de acción; anticipación y prevención; eficiencia y sostenibilidad en el uso de los recursos, y resiliencia (o capacidad de resistencia y recuperación).
- Ocho *entornos*: Unión Europea (UE); Mediterráneo; América Latina; Estados Unidos y relación trasatlántica; África (Sahel, Cuerno de África y golfo de Guinea como áreas de especial interés); Asia y Australia; Rusia; ONU, OTAN y otros foros multilaterales.
- Doce *riesgos y amenazas*: conflictos armados; terrorismo; ciberamenazas; crimen organizado; inestabilidad económica y financiera; vulnerabilidad energética; proliferación de armas de destrucción masiva; flujos migratorios irregulares; espionaje; emergencias y catástrofes; vulnerabilidad del espacio marítimo, y vulnerabilidad de las infraestructuras críticas (instalaciones, redes, sistemas y equipos físicos y lógicos) para la prestación de servicios esenciales en sectores estratégicos (Administración Pública, agua, alimentación, energía, espacio, industria química, nuclear, investigación, salud, sistema financiero y tributario, tecnologías de la información y las comunicaciones (TIC) y transportes).
- Seis *factores potenciadores*, aquellos que sin ser en sí mismos un riesgo o amenaza pueden actuar como desencadenantes o agravantes: cambio climático; pobreza; desigualdad; extremismos ideológicos; desequilibrios demográficos, y generalización del uso nocivo de las nuevas tecnologías.
- Doce *ámbitos de actuación* —que se corresponden con los riesgos y amenazas— cada uno de ellos con su respectivos *objetivos* y principales *líneas de acción*: defensa nacional; lucha contra el terrorismo; ciberseguridad; lucha contra el crimen organizado; seguridad económica y financiera; seguridad energética; no proliferación de armas de destrucción masiva; ordenación de flujos migratorios; contrainteligencia; protección ante emergencias y catástrofes; seguridad marítima, y protección de las infraestructuras críticas.
- Ocho *principios sustentadores* de un Sistema de Seguridad Nacional: liderazgo por el presidente del Gobierno; funcionamiento integrado y coordinado de las Administraciones Públicas competentes; optimización de recursos; modernización de estructuras y procedimientos de actuación; implicación de la sociedad civil y fomento de una cultura

de seguridad; colaboración público-privada; gestión de la información y del conocimiento, y transparencia.

La *estructura orgánica* o arquitectura de gobernanza de este Sistema de Seguridad Nacional incluye, en aras a la flexibilidad requerida por la cuestión, un Consejo de Seguridad Nacional (como máximo órgano colegiado del Gobierno) y diferentes comités especializados (en apoyo al Consejo en su ámbito de actuación), uno de los cuales es un Comité Especializado de Situación para la gestión de situaciones de crisis que excedan un ámbito particular de especialización.

La ESN reconoce explícitamente el carácter dinámico y continuo en el tiempo del proceso de revisión estratégica y contempla una adaptación del marco normativo, para lo cual el Consejo de Seguridad Nacional ha elaborado un anteproyecto de ley que fue debatido en el Consejo de Ministros el 16 de enero de 2015, y cuyo proyecto ha sido remitido a las Cortes Generales según lo acordado por el Consejo de Ministros de 22 de mayo, por lo que a fecha de redacción de este artículo se encuentra en tramitación parlamentaria. Cuatro son los títulos del proyecto, dedicados respectivamente a: I. Órganos competentes de la Seguridad Nacional; II. Sistema de Seguridad Nacional; III. Gestión de crisis, y IV. Contribución de recursos a la Seguridad Nacional.

La Estrategia de Ciberseguridad Nacional

Como objetivo global en materia de ciberseguridad, la ESN marca el «garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques», que tienen las siguientes cuatro características singulares que contribuyen a su proliferación: bajo coste, ubicuidad y fácil ejecución, efectividad e impacto y reducido riesgo para el atacante. En su logro, el desarrollo de un marco normativo —políticas, procedimientos y normas técnicas—, la generación de confianza y el respeto a la diversidad y neutralidad tecnológica y a los derechos fundamentales son consideraciones relevantes que toma en cuenta la Estrategia de Ciberseguridad Nacional.

Así, su *propósito* es fijar las directrices del uso seguro del ciberespacio, para lo que establece cuatro *principios rectores* alineados con los principios informadores de la ESN —liderazgo nacional y coordinación de esfuerzos; responsabilidad compartida; proporcionalidad, racionalidad y eficacia, y cooperación internacional— y un desglose del objetivo global en seis *objetivos específicos*: I) garantizar el adecuado nivel de ciberseguridad y resiliencia de los sistemas TIC que utilizan las Administraciones Públicas; II) impulsar la ciberseguridad y resiliencia de los sistemas TIC usados por el sector empresarial en general (con especial atención en la protección del Patrimonio Tecnoló-

gico de España) y los operadores de infraestructuras críticas en particular; III) potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio; IV) sensibilizar a la sociedad de los riesgos derivados del ciberespacio; V) fomentar la cualificación en materia de ciberseguridad, y VI) contribuir a la mejora de la ciberseguridad en el ámbito internacional.

Para la consecución de los objetivos señalados, y conforme a lo establecido en la ESN, la orientación de la acción en materia de ciberseguridad se articula a través de las ocho siguientes *líneas*: 1) capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas; 2) seguridad de los sistemas TIC que soportan las Administraciones Públicas; 3) seguridad de los sistemas TIC que soportan las infraestructuras críticas; 4) capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia; 5) seguridad y resiliencia de las TIC en el sector privado; 6) conocimientos, competencias e I + D + i; 7) cultura de la ciberseguridad, y 8) compromiso internacional.

La Estrategia de Seguridad Marítima Nacional

Múltiples iniciativas internacionales constatan la importancia de la seguridad marítima, que para el caso de España se acentúa por nuestra configuración geográfica, dimensión socioeconómica e implicación en flujos marítimos, afectando a una pluralidad de *intereses nacionales* que incluye: cumplimiento de la legislación nacional y del Derecho Internacional; protección de la vida humana en el mar; libertad y seguridad de navegación; comercio y transporte marítimos; industria naviera y otras industrias marítimas; seguridad de buques bajo pabellón español; puertos e infraestructuras marítimas; recursos del medio marino; medio ambiente marino, y patrimonio arqueológico subacuático.

Por las características propias del medio, los *riesgos y amenazas* requieren en este caso una taxonomía *ad hoc*, y así cabe clasificarlos en dos grandes grupos según su origen sea intencionado o fortuito: *actos ilícitos contra la seguridad marítima* (entre los que se incluyen: tráficos ilícitos —de difícil control por el uso creciente y generalizado de contenedores—; piratería; terrorismo; proliferación de armas de destrucción masiva; inmigración irregular y tráfico ilícito de migrantes; explotación ilegal de recursos marinos —vivos, como la pesca, y no vivos, como los energéticos— y destrucción y degradación del medio marino; actos contra el patrimonio cultural subacuático, y ciberamenazas a sistemas de vigilancia y control, infraestructuras marítimas críticas y sistemas de navegación y comunicación), y *accidentes marítimos y catástrofes naturales*. Como *factores potenciadores* específicos de lo marítimo, citar los que representan el régimen de libertades del mar, lo extenso del medio marino y las delimitaciones marítimas pendientes.

Establecido como *objetivo* en el ámbito de la seguridad marítima el impulso de una política amplia de seguridad con la finalidad de proteger los intereses marítimos nacionales ya citados, la Estrategia de Seguridad Marítima Nacional marca actuaciones orientadas por los principios informadores de la ESN en cada una de las siguientes cinco *líneas de acción*: I) adopción de un enfoque integral que potencie la actuación coordinada y cooperativa de las diferentes administraciones implicadas; II) adopción de medidas para la optimización en el uso de los recursos; III) fomento de la cooperación internacional; IV) fomento de la colaboración en el sector privado, y V) mejora de la ciberseguridad en el ámbito marítimo.

La Estrategia de Seguridad Energética Nacional

Dependencia, diversificación y baja conectividad —por nuestra condición de «isla energética» resultante de la insuficiente conexión con el resto de Europa— son los rasgos que definen el sistema energético español. Necesariamente enmarcada en el contexto de la UE, e inmersa en el proceso de integración física y regulatoria que constituye la construcción del Mercado Interior de la Energía, cuatro son los *vectores*, a menudo divergentes, que orientan su seguridad: suministro (regular y de calidad), abastecimiento, sostenibilidad económica y sostenibilidad medioambiental.

Se concibe por tanto la seguridad energética nacional, desde una perspectiva de bien público, como «la acción del Estado orientada a garantizar el suministro de energía de manera sostenible económica y medioambientalmente, a través del abastecimiento exterior y la generación de fuentes autóctonas, en el marco de los compromisos internacionales asumidos», en la cual se identifican cinco *retos*: el cambio climático y la degradación ambiental; el crecimiento de la demanda (liderado por economías emergentes como China e India); la volatilidad de los mercados energéticos (y su fraccionamiento y escasa integración, en el caso de la UE); la gestión eficaz de las reservas estratégicas (principal herramienta de seguridad para el caso de recursos almacenables de los que se depende), y la cultura de seguridad energética.

Los *riesgos y amenazas* se desagregan en diferentes perspectivas: *económica* (inversiones inadecuadas en infraestructuras; actividades fraudulentas), *geoestratégica* (inestabilidad política en países productores; diversificación de recursos; amenazas a las rutas de aprovisionamiento; conflictos políticos entre países productores, consumidores y de tránsito), *técnica* (insuficientes interconexiones; mantenimiento inadecuado de infraestructuras; riesgos operativos) y *medioambiental* (catástrofes). Y por supuesto, entre las amenazas cabe considerar las *deliberadas*, ya sean físicas sobre las infraestructuras críticas como cibernéticas.

Al *objetivo final* marcado por la ESN de diversificar las fuentes de energía, garantizar la seguridad del transporte y abastecimiento e impulsar la sostenibilidad, la Estrategia de Seguridad Energética Nacional añade nueve *objetivos parciales* con sus correspondientes *líneas de acción*: 1) contribuir al fortalecimiento de la seguridad energética en el conjunto de la UE; 2) asegurar la adecuada diversificación del *mix* energético; 3) seguridad de abastecimiento; 4) fomento de fuentes autóctonas en aras a la diversificación del *mix* y disminución de la dependencia; 5) favorecimiento de la sostenibilidad económica y medioambiental; 6) promoción de la seguridad de las infraestructuras frente a accidentes de origen técnico o errores humanos y catástrofes naturales; 7) protección de infraestructuras físicas frente a amenazas deliberadas físicas o cibernéticas; 8) garantizar la seguridad en el transporte, tanto terrestre como marítimo, y 9) fomentar una cultura de seguridad energética.

La dimensión tecnológica (I + D + i), las intervenciones por el lado de la demanda (eficiencia energética) y las medidas medioambientales (compromisos europeos en materia de reducción de emisiones e instrumentos asociados, como el sistema de comercio de emisiones) forman parte de la panoplia de actuaciones.

Comentar como fortaleza en materia de seguridad energética que, en el contexto actual del panorama energético mundial, España cuenta con una situación geográfica óptima para convertirse en el *hub* energético del sur de Europa. En efecto, nos encontramos por un lado en el centro de gravedad de la nueva oferta energética procedente de los países norteamericanos (que están liderando la revolución de los hidrocarburos no convencionales), los latinoamericanos (con los que nos unen vínculos históricos), el golfo de Guinea y el norte de África. Y por otro lado, contamos con un desarrollo tal de infraestructuras energéticas (plantas de regasificación de gas natural licuado y refinerías) que, con la salvedad ya apuntada de la insuficiencia de interconexiones a través de los Pirineos, nos postulan como punto de entrada ideal para suministros que supongan una alternativa a los procedentes de Rusia, de cuya dependencia energética la UE acumula experiencias poco agradables en las recurrentes crisis Rusia-Ucrania que tienen lugar cada invierno cuando las necesidades de gas natural para su uso en calefacción son máximas.

Intereses esenciales, capacidades industriales y áreas de conocimiento

Por su actualidad y por afectar de pleno a la ciberseguridad y seguridad marítima, y antes de cerrar el artículo con unas conclusiones, parece oportuno hacer referencia a los conceptos que incluye el título de este apartado y que se pueden considerar una excepción al enfoque transnacional de la seguridad.

En el marco de la ESN se entiende por «interés esencial de seguridad» aquel cuya protección sea prioritaria para el desarrollo de las líneas de acción

INTERESES ESENCIALES DE SEGURIDAD EN EL ÁMBITO DE LA DEFENSA NACIONAL: EL APOYO A UNA BASE TECNOLÓGICA E INDUSTRIAL NACIONAL Y LAS CAPACIDADES INDUSTRIALES

ÁREAS DE CONOCIMIENTO	SUPUESTOS DE PROTECCIÓN	ASPECTOS ESENCIALES A PROTEGER
a) Mando y control, comunicaciones, información (C4i). b) Ciberdefensa. c) Vigilancia, reconocimiento, inteligencia y adquisición de objetivos (ISTAR). d) Control de tráfico y de ayudas a la navegación. e) Sistemas críticos embarcados en plataformas. f) Sistemas espaciales, de tratamiento de datos y de misión. g) Simulación de equipos y sistemas de armas para entrenamiento avanzado. h) Sistemas de navegación, control de guiado y carga de pago en misiles y municiones complejas. i) Sistemas complejos integrados por otros sistemas de armas avanzados cuyos requisitos de integración están vinculados a intereses esenciales de defensa y seguridad.	a) Cuando la capacidad que se necesite se refiera a la seguridad de la información y las comunicaciones estratégicas de España. b) Cuando la operatividad de una capacidad española dependa del acceso a información de inteligencia o tecnologías clasificadas. c) Cuando las circunstancias operativas impongan cambios en una capacidad española en servicio que solo pueda ser respondida con unos niveles muy altos de disponibilidad y agilidad en el suministro. d) Cuando para la obtención de una ventaja operacional de nuestras Fuerzas Armadas dependa del aseguramiento de uno o más aspectos del funcionamiento de una capacidad. e) Cuando la efectividad de una capacidad militar dependa: 1. De la posibilidad de mejorar su eficacia a través de la integración de sistemas y de la comprensión del sistema como un todo. 2. De asegurar el funcionamiento y acceso libre a subsistemas críticos. f) Aquellas otras que se puedan determinar por el Gobierno.	a) Las habilidades y conocimientos esenciales para diseñar, desarrollar, integrar, evaluar, apoyar y mantener sistemas y subsistemas claves, junto con la realización de pruebas, evaluación, y procesos de mantenimiento y modernización de los mismos. b) Las instalaciones e infraestructuras que den soporte a lo anterior. c) Las tecnologías críticas para el diseño y desarrollo de las capacidades descritas en el apartado Primero de este acuerdo. d) El acceso apropiado al uso de tecnologías que permita a España y sus suministradores mantener, modernizar y operar sistemas y subsistemas claves. e) Actividades de investigación y desarrollo tecnológico o de innovación, de aplicación directa o indirecta a las áreas de conocimiento y capacidades industriales estratégicas de interés para la defensa y la seguridad.

Fuente: Acuerdo del Consejo de Ministros de 29 de mayo de 2015 (BOE 6 de agosto de 2015).

estratégicas y el cumplimiento de los objetivos establecidos en los distintos ámbitos de actuación. Como elemento primordial de Seguridad Nacional, la Defensa Nacional debe proveerse de *capacidades* para proteger estos intereses esenciales en atención a los principios de *ventaja operacional* y *libertad de acción* en casos de amenazas no compartidas. Y entre dichas capacidades, además de otros factores como la inteligencia, la formación o la doctrina, destacan las materiales referidas a equipos, sistemas y servicios, cuya adquisición se ha de hacer en aplicación ponderada de los principios *finalista*, de *eficiencia* y, excepcionalmente y cuando se afecten a los intereses esenciales de seguridad, *soberanía*, lograda esta última mediante medidas de protección en apoyo a una *base tecnológica e industrial nacional*.

En cumplimiento de lo establecido en la Ley 24/2011 de Contratos del Sector Público en los ámbitos de la Defensa y de la Seguridad, por Acuerdo del Consejo de Ministros de 29 de mayo de 2015 se han establecido las «áreas de conocimiento» que afectan a los intereses esenciales de seguridad y defensa, se han tasado los *supuestos* que en un análisis, caso por caso, podrán dar lugar a acciones de protección y se han definido las «capacidades industriales» específicas que en relación con las áreas de conocimiento merecen protección.

Conclusiones

¿Tienen algo en común los ámbitos de seguridad cibernético, marítimo y energético cuyas estrategias se han sintetizado? Desde luego que sí, y veámoslo con un ejemplo.

En el *mix* energético español tienen aún un peso más que relevante los combustibles fósiles. Salvo el caso del carbón, en el que una parte del abastecimiento es de origen doméstico, la dependencia de las importaciones es plena. Dichas importaciones se realizan en el caso del petróleo y sus derivados —de los que depende como fuente propulsora nuestro sistema de transporte, incluido el marítimo— en su totalidad por vía marítima (en buques petroleros).

En el caso del gas natural, aproximadamente las dos terceras partes llega también por vía marítima (en buques metaneros, en forma de gas natural licuado-GNL, que se descarga en las plantas de regasificación para su inyección en el sistema) y la tercera parte restante lo hace a través de infraestructuras de transporte que por el lecho marino cruzan el estrecho de Gibraltar (caso del gasoducto del Magreb, con origen en Argelia y tránsito a través de Marruecos) o entran por la costa almeriense (caso del gasoducto MEDGAZ, directamente desde su origen en los yacimientos argelinos, sin tránsito por tanto por terceros países).

Los tránsitos marítimos de hidrocarburos se producen a menudo a través de puntos críticos como pasos estrechos de alta densidad y alta vulnerabilidad

(*choke-points,* como el canal de Suez o los estrechos de Ormuz o del Bósforo y los Dardanelos), lo que obliga, en ausencia de seguridad marítima y en aras a la cobertura de riesgos de ruptura de suministro, al almacenamiento de reservas de seguridad en instalaciones que por su naturaleza y finalidad se convierten en infraestructuras críticas.

La operación de estas y de otras infraestructuras similares, como los gaseoductos mencionados o la interconexión eléctrica España-Marruecos o la de la península con Baleares, se hace a través de sofisticados sistemas TIC, sometidos a las ciberamenazas que les son propias, dependientes para su funcionamiento de un suministro energético fiable y asimismo indispensables para la seguridad marítima.

El ejemplo describe un panorama de interdependencias en el que se solapan riesgos cubiertos en las tres estrategias de seguridad descritas: la de ciberseguridad, la marítima y la energética. Y es muy ilustrativo del carácter integral del problema de la Seguridad Nacional, detrás del cual se encuentra la motivación última del ejercicio de análisis estratégico que representa la ESN y sus diferentes estrategias específicas que se vienen desarrollando.

Como comentario final, apuntar que un reto horizontal que afecta al problema de la seguridad es el de la necesidad de implicación ciudadana, siendo la concienciación y creación de una «cultura de seguridad» un aspecto clave para el cual este artículo ha pretendido ser una modestísima contribución.

BIBLIOGRAFÍA

Estrategia de Seguridad Nacional. Un proyecto compartido. Departamento de Seguridad Nacional. Presidencia del Gobierno. 2013. *http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf*

Estrategia de Ciberseguridad Nacional. Departamento de Seguridad Nacional. Presidencia del Gobierno. 2013. *http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf*

Estrategia de Seguridad Marítima Nacional. Departamento de Seguridad Nacional. Presidencia del Gobierno. 2013. *http://www.lamoncloa.gob.es/documents/20131333estrategiadeseguridadmartima_u.pdf*

Estrategia de Seguridad Energética Nacional. Departamento de Seguridad Nacional. Presidencia del Gobierno. 2015. http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/Documents/EST*RATEGIA%20DE%20SEGURIDAD%20ENERG%C3%89TICA%20NACIONAL%20(WEB).pdf*

Proyecto de Ley de Seguridad Nacional. Boletín Oficial de las Cortes Generales. 29 de mayo de 2015. *http://www.congreso.es/public_oficiales/L10/CONG/BOCG/A/BOCG-10-A-158-1.PDF*

Resolución 420/38100/2015, de 30 de julio, de la Secretaría General Técnica, por la que se publica el Acuerdo del Consejo de Ministros de 29 de mayo de 2015, por el que se determinan las capacidades industriales y áreas de conocimiento que afectan a los intereses esenciales de la Defensa y la Seguridad Nacional. http://www.boe.es/boe/dias/2015/08/06/pdfs/BOE-A-2015-8843.pdf