CONTRIBUCIÓN DEL MINISTERIO DEL INTERIOR EN LAS LÍNEAS DE ACCIÓN DE LA ESTRATEGIA DE SEGURIDAD NACIONAL ESPAÑOLA

FERNANDO MOURE COLÓN

"La Estrategia de Seguridad Nacional 2013 es un paso trascendente. Continúa y revisa la Estrategia Española de Seguridad aprobada en 2011, adaptando y actualizando su contenido a los cambios del escenario estratégico, configurando un nuevo Sistema de Seguridad Nacional e implicando a la sociedad civil en los ámbitos de interés prioritario de la Seguridad Nacional"

Mariano Rajoy, Presidente del Gobierno español, 31 de mayo de 2013

RESUMEN

El Consejo de Ministros aprobó el 31 de mayo de 2013 la Estrategia de Seguridad Nacional (ESN). La Estrategia se centra en el enfoque integral de la Seguridad Nacional, refleja los riesgos y amenazas que son necesarios encarar en un mundo que está cambiando profunda y constantemente. En total, la Estrategia contempla hasta doce amenazas: conflictos armados; terrorismo; ciberamenazas; crimen organizado; inestabilidad económica y financiera; vulnerabilidad energética; flujos migratorios irregulares; armas de destrucción masiva; espionaje; emergencias y catástrofes naturales; vulnerabilidad del espacio marítimo y vulnerabilidad de las infraestructuras críticas y servicios esenciales.

La ESN establece para cada una de las amenazas enumeradas, "doce ámbitos prioritarios de actuación", en cada uno de los cuales puede apreciarse el objetivo a alcanzar y varias líneas de acción estratégicas. El desarrollo específico de estas líneas de acción para cada ámbito constituye un gran reto para el nuevo sistema de Seguridad Nacional.

En este trabajo el lector podrá conocer la contribución del Ministerio del Interior en las líneas de acción de la ESN española (lucha contra el terrorismo, la ciberseguridad, la lucha contra el crimen organizado, la ordenación de flujos migratorios, etc.), que con su estructura está preparado para afrontar las medidas concretas que le asignen. Las tareas del Ministerio del Interior están relacionadas de alguna forma con los ámbitos descritos y las Fuerzas y Cuerpos de Seguridad del Estado (Guardia Civil y el Cuerpo Nacional de Policía) cuentan con capacidad en recursos materiales y humanos para contribuir en las líneas de acción expuestas.

Palabras clave: Estrategia de Seguridad Nacional; riesgos; amenazas; Ministerio del Interior; Guardia Civil.

ABSTRACT

The Council of Ministers on May 31, 2013, approved the National Security Strategy (ESN). The Strategy focuses on the comprehensive approach to national security, reflects the risks and threats that are needed to face in a world that is deep and constantly changing. Overall, the strategy includes up to twelve threats: armed conflicts,

terrorism, cyber threats, organized crime, economic and financial instability, energy vulnerability, irregular migration, weapons of mass destruction, espionage, emergencies and natural disasters, vulnerability of maritime space and vulnerability of critical infrastructure and essential services.

The ESN sets for each of the listed threats, "Twelve priority areas", each of which can appreciate the aim to reaching and several action lines. The specific development of these action lines for each area is a great challenge for the new system of National Security.

In this paper the reader will know the contribution of the Ministry of Interior in the action lines of the Spanish National Security Strategy, (fight against terrorism, cyber security, the fight against organized crime, the management of migratory flows, etc.), which its structure is prepared to meet the specific measures assigned. The tasks of the Ministry of Interior are related in some way to the areas described and the State security forces (Guardia Civil and the National Police), those with ability in material and human resources to assist in the action lines set out above.

Key words: National Security Strategy; risks; threats; Ministry of Interior; Guardia Civil.

1. INTRODUCCIÓN

Siguiendo la estela de las publicaciones de la Estrategia de Seguridad Europea ESS-2003 (European Security Strategy)[1] y de las estrategias de seguridad nacionales de Estados Unidos, Reino Unido, Alemania, Holanda y Francia entre otras, en España aparecen los primeros compromisos del Gobierno durante 2008, para afrontar los nuevos retos de seguridad que afectan a los ciudadanos. De esta forma en las posteriores comparecencias de los ministros de Defensa e Interior[2], explicaban el nuevo escenario en el que a las tradicionales demandas de seguridad, aparecen otras graves amenazas como el terrorismo internacional, la criminalidad organizada, los grandes movimientos de inmigración ilegal, el tráfico de armas de destrucción masiva o las catástrofes medioambientales, entre otras. Ante estos desafíos hace falta una respuesta del conjunto de las instituciones del Estado, por lo que el Gobierno se comprometió en elaborar una estrategia nacional de seguridad. Ya anteriormente la Directiva de Defensa Nacional[3] (DDN-2008), donde expresaba "la necesidad de una estrategia de seguridad nacional, resulta evidente", en la que

1 La difusión de la "cultura de seguridad" puede contribuir en la promoción de la participación ciudadana, fomentando la transparencia y aumentando la intercomunicación para evitar alguna de las amenazas descritas en la ESN.

2 España, Congreso de los Diputados. (27 de mayo de 2008). Comparecencia del ministro de Interior, para informar sobre las líneas generales de la política de su departamento. (pp. 2-3). Recuperado el 20 de septiembre de 2013) del sitio web: http://www.congreso.es/public_oficiales/L9/CONG/DS/CO/CO_029.PDF

3 España, Consejo Defensa Nacional. (30 de diciembre de 2008). Directiva de Defensa Nacional 01/2008. (p. 1). Recuperado el 20 de abril de 2013, del sitio web: <http://www.centredelas.org/images/stories/adjunts/511_ddn_1-2008.pdf> Primera que se aprueba bajo la vigencia de la Ley Orgánica 5/2005, de la Defensa Nacional, fue sancionada por el presidente del Gobierno el 30 de diciembre de 2008. Las DDN de 1980, 1984 y 1986 están clasificadas; las 1992, 1996, 2000, 2004, 2008 y 2012 son documentos sin clasificar.

se integrarán las distintas estrategias sectoriales que hasta ese momento convivían separadas, intentando asegurar una coherencia y coordinación interministerial con un enfoque amplio.

En diciembre de 2009 el Gobierno constituye un grupo interministerial bajo la dirección de Javier Solana, ex Secretario General de la OTAN y ex alto Representante de la Política Exterior y de Seguridad común de la UE, y después de un largo proceso de elaboración, en el Consejo de Ministros del día 24 de junio de 2011, fue aprobada la Estrategia Española de Seguridad[4] (EES), "una responsabilidad de todos", constituyendo un hito en la historia del planeamiento estratégico de España. Después, en agosto de 2012, el Gobierno empezó la adaptación del contenido de la mencionada estrategia, a los cambios derivados del escenario actual y situación económica. Para la elaboración del borrador de la nueva estrategia hicieron falta varias reuniones[5], presididas por Emilio Lamo de Espinosa, a la que asistieron por parte del Ejecutivo del Gobierno de Rajoy, Jorge Moragas (anterior interlocutor con Solana en 2011) y Alfonso de Senillosa; por parte del PSOE asistieron el diputado José Enrique Serrano (ex jefe de gabinete de Felipe González y de Zapatero), además de Narcís Serra (ex ministro de Defensa y Vicepresidencia). También participó Antonio Camacho (ex secretario de Estado de Seguridad) y Diego López Garrido (portavoz de Defensa del Grupo Socialista). Con estas reuniones se consiguió un alto nivel de consenso, manteniendo las líneas generales de la anterior estrategia, se acortó el texto y se consiguió una mejor lectura para lograr su máxima difusión, concluyendo sus trabajos con la aprobación por el Consejo de Ministros[6] del 31 de mayo de 2013, de una nueva Estrategia de Seguridad Nacional, "un proyecto compartido" (ESN-2013)[7] y del Real Decreto que regula el Consejo de Seguridad Nacional.

Según el resumen del Consejo de Ministros antes citado, la ESN-2013, se centra en el enfoque integral de la seguridad nacional, refleja los riesgos y amenazas que son necesarios encarar en un mundo que está cambiando profunda y constantemente. También contempla el concepto de seguridad de una manera amplia acorde con estas transformaciones globales que afectan al Estado y a la vida diaria del ciudadano. De esta forma con el objetivo de analizar las amenazas y riesgos de la seguridad en España, tanto interior como exterior, así como evaluar sus capacidades de respuesta y establecer unas líneas de acción concretas, la ESN-2013 busca un entorno seguro para contribuir al bienestar, progreso y prosperidad, estableciendo "doce ámbitos prioritarios de actuación".

4 España, Presidencia del Gobierno. (30 de junio de 2011). Estrategia Española de Seguridad. Una responsabilidad de todos (EES). (pp. 1-6). Recuperado el 9 de marzo de 2013, del sitio web: http://www.urjc.es/ceib/investigacion/publicaciones/REIB_05_01_Document03.pdf

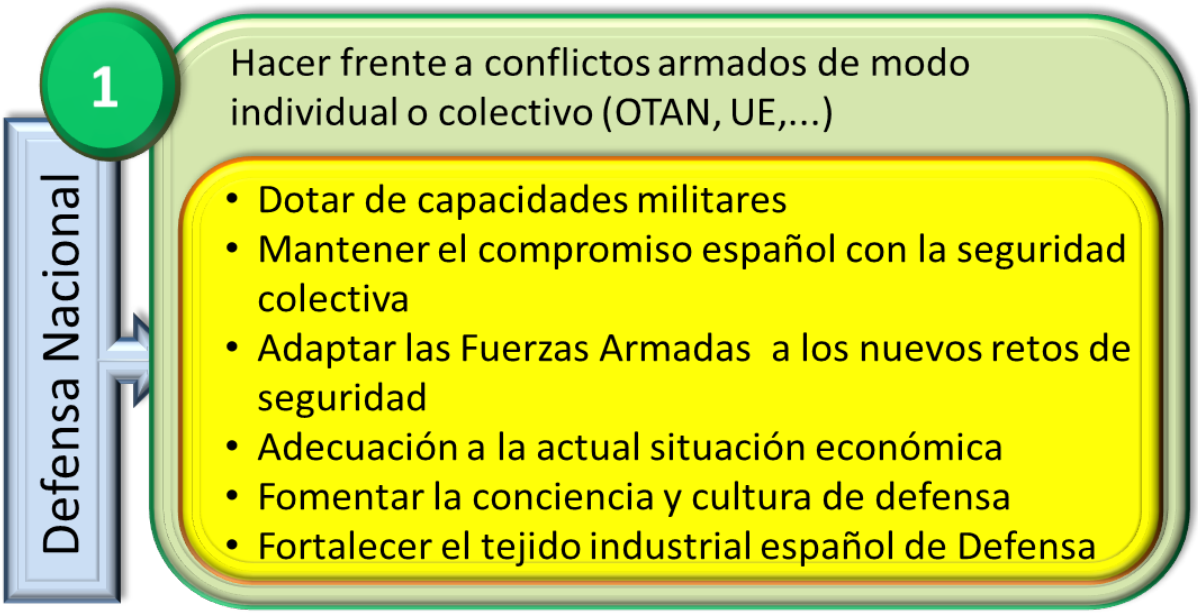
5 Prensa digital "El Confidencial", Noticias. (1 de junio de 2013). Primer acuerdo del Gobierno con el PSOE desde principios de la legislatura sobre la Estrategia de Seguridad Nacional. Recuperado el 4 de septiembre de 2013, del sitio web: http://www.elconfidencial.com/espana/2013/06/01/el-gobierno-pacta-con-el-viejo-psoe-la-estrategia-de-seguridad-nacional-122142/

6 España, Consejo de Ministros. (31 de mayo de 2013). Nota de prensa: Aprobada la Estrategia de Seguridad Nacional de 2013. Recuperado el 1 de septiembre de 2013, del sitio web: http://www.lamoncloa.gob.es/ConsejodeMinistros/Enlaces/310513Enlace++seguridad.htm

7 España, Presidencia del Gobierno. (31 de mayo de 2013). Estrategia de Seguridad Nacional. Un proyecto compartido. (pp. 53-58). Recuperado el 8 de junio de 2013, del sitio web: http://www.lamoncloa.gob.es/NR/rdonlyres/0BB61AA9-97E5-46DA-A53E-DB7F24D5887D/0/Seguridad_1406connavegacionfinalaccesiblebpdf.pdf

A continuación vamos a analizar brevemente cada uno de los doce ámbitos de actuación, en los que se puede apreciar en cada punto, el objetivo a alcanzar y varias líneas de acción estratégicas, además de la contribución o participación concreta del Ministerio del Interior español.

2. DEFENSA NACIONAL



Obviamente el peso específico en este ámbito corresponde al Ministerio de Defensa, y en este caso el contenido de la ESN-2013 excede del ámbito estricto de las competencias del Ministerio del Interior, pero es evidente que las tareas del Ministerio del Interior y de la Secretaría de Estado de Seguridad caen todas ellas bajo lo que sistematiza la estrategia en cualquiera de sus ámbitos.

En este sentido la Ley Orgánica de la Defensa Nacional[8], especifica claramente que la ejecución de la política de defensa corresponde al ministro de Defensa (art. 7), pero el ministro del Interior forma parte del Consejo de Defensa Nacional (art. 8.5) y en la Comisión Interministerial de Defensa participa también un representante del Ministerio del Interior y un Oficial General de la Guardia Civil, contribuyendo en la coordinación de los órganos que integran el Sistema Nacional de Conducción de Situaciones de Crisis.

Los retos de seguridad en este ámbito, están ligados con las capacidades de defensa y éstas necesariamente están unidas a la seguridad colectiva de la Unión Europea (UE), que establece en su Tratado[9] (TUE, artículo 42, apartado 2, primer párrafo), la Política Común de Seguridad y Defensa (PCSD), que incluye la definición progresiva de una política común de defensa de la Unión, dirigida por unanimidad por el Consejo Europeo, quién recomendará a los estados miembros que adopten una decisión de

8 Vid. Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional. Publicada en BOE nº 276 de 18 de noviembre de 2005.

9 Modificado por el apartado 25) del artículo 1 del Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea (DOUEC, nº 306 de 17 diciembre de 2007).

conformidad con sus respectivas normas constitucionales. Hoy por hoy[10] no existe un mecanismo de defensa común que plantee obligaciones irrenunciables de proporcionar fuerzas para la ejecución de la PCSD, por lo que España debe esforzarse por encontrar socios para actuar activamente para defender sus intereses y garantizar la seguridad de los españoles.

Esta garantía de la seguridad de los españoles, también es citada en la Directiva de Defensa Nacional[11] (2012) como "una responsabilidad y obligación inalienable, intransferible e irrenunciable del Gobierno de la nación. La política de defensa y la capacidad de las Fuerzas Armadas para prevenir, disuadir y responder, ante acciones que ponga en peligro nuestra seguridad, conforman la columna vertebral del sistema institucional de nuestra defensa".

Siguiendo con el ámbito de la Defensa Nacional y cambiando de línea de acción, desde el punto de vista del Ministerio de Defensa, corresponde a la Secretaría General de Política de Defensa (SEGENPOL), la política cultural de seguridad y defensa y la promoción de la conciencia de defensa nacional[12], contando con el Instituto Español de Estudios Estratégicos (IEEE) del Centro Superior de Estudios de la Defensa Nacional (CESEDEN). Por otra parte, y relacionada con línea de acción de la conciencia y cultura de seguridad, el 18 de junio 2013, comparece ante la Comisión de Interior del Congreso de los Diputados, el Secretario de Estado de Seguridad del Ministerio del Interior (SES), Francisco Martínez Vázquez[13], para informar sobre los desafíos actuales, incardinados en el esquema de prioridades que el ministro del Interior, Jorge Fernández Díaz[14], presentó anteriormente ante la misma Comisión el 31 de enero de 2012. El SES centró su intervención en ocho ejes estratégicos que constituyen los desafíos de seguridad en España, entre ellos su "eje estratégico7" que detalla la participación ciudadana:

El esfuerzo por acercar las tareas de seguridad a los ciudadanos y crear esa "cultura de seguridad" se impulsa no sólo promoviendo la participación ciudadana en asuntos como los distintos planes de seguridad, sino también fomentando una mayor transparencia en el trabajo de las fuerzas policiales…, uno de los objetivos estratégicos del Ministerio del Interior es acercar a los ciudadanos a la labor desempeñada por las Fuerzas y Cuerpos de Seguridad del Estado (FCSE). Para ello, se han puesto a

10 Golmayo Fernández, P. (2013). Condicionamientos y compromisos, capítulo primero. En Escuela de Altos Estudios de la Defensa, EALEDE, Enfoque multinacional al desarrollo de capacidades de Defensa. La Smart defence de la OTAN frente al Pooling Sharing de la UE. Documento de Seguridad y Defensa nº 56 (págs. 37-40). Madrid: Ministerio de Defensa.

11 España, Presidencia del Gobierno. (31 de julio de 2012). Directiva Defensa Nacional 2012. Por una defensa necesaria, por una defensa responsable. (pp. 2-3). Recuperado el 20 de abril de 2013, del sitio web: http://www.defensa.gob.es/Galerias/politica/seguridad-defensa/ficheros/DGL-DirectivaDefensaNacional-2012.pdf

12 Casas Álvarez, F. J. (8 de julio de 2013). La cultura de seguridad y defensa comienza en la escuela. Revista española de Defensa, nº 297. (pp. 14-15). Recuperado el 6 de septiembre de 2013, del sitio web: http://www.defensa.gob.es/Galerias/politica/seguridad-defensa/ficheros/red-297-cultura-seguridad-nacional.pdf

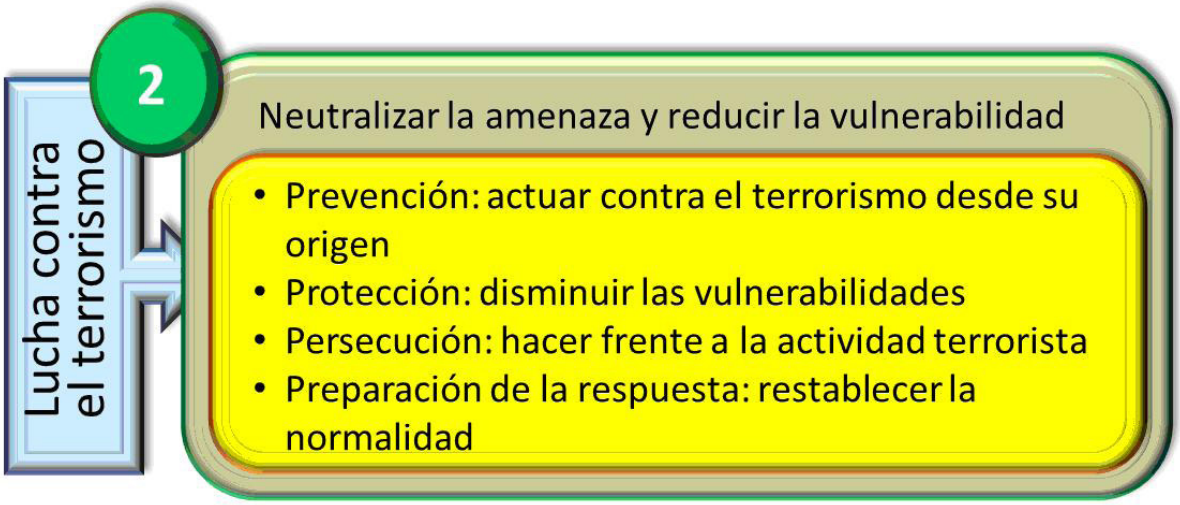
13 España, Comisión de Interior del Consejo de los Diputados. (18 de junio de 2013). Comparecencia del Secretario de Estado de Seguridad, para informar sobre las líneas generales de la SES del Ministerio del Interior. (pp. 2, 18-19). Recuperado el 3 de agosto de 2013, del sitio web: http://www.interior.gob.es/file/61/61735/61735.pdf

14 España, Congreso de los Diputados. (31 de enero de 2012). Comparecencia del ministro de Interior, para informar sobre las líneas generales de la política de su departamento. (pp. 2-11). Recuperado el 10 de septiembre de 2013) del sitio web: http://www.congreso.es/public_oficiales/L10/CONG/DS/CO/CO_029.PDF

disposición de los ciudadanos diversos canales de información y medios ágiles de intercomunicación que permiten, entre otras funciones, denunciar actividades delictivas de forma segura y confidencial…

En este sentido es interesante conocer que la anterior línea de acción es también un objetivo del Centro de Análisis y Prospectiva de la Guardia Civil (CAP), que destaca el papel indudable de la Guardia Civil como difusor de la cultura de seguridad[15].

3. LUCHA CONTRA EL TERRORISMO



El Ministerio del Interior[16] tiene como primer objetivo el garantizar a todos los ciudadanos el pleno disfrute de sus derechos y libertades, libre de la violencia terrorista o de su amenaza, por lo que marca una primera línea de acción en el desarrollo de una estrategia antiterrorista integral que permita responder eficazmente a los riesgos y amenazas a los que debe hacer frente nuestro país. España debe hacer frente a los riesgos derivados del terrorismo nacional e internacional en tres puntos concretos: primero, desarrollar la estrategia nacional de ciberseguridad de manera que se articulen los mecanismos precisos para hacer frente a esta amenaza creciente y en particular contra el ciberterrorismo; segundo, fomentar las acciones precisas a perfeccionar por parte del Estado dirigidas a impedir procesos de radicalización a través de la implantación de un plan de lucha contra la radicalización que requerirá de la cooperación y colaboración de otras administraciones públicas; tercero, desarrollar en el marco de las iniciativas de la Unión Europea un plan específico de actuación y cooperación en la lucha contra el terrorismo internacional en el área del Magreb-Sahel, confeccionar un plan integral de lucha contra la financiación del terrorismo internacional, mejorar la capacidad de prevención de atentados terroristas, así como la preparación para hacer frente a amenazas emergentes, como el empleo de material de tipo nuclear, radiológico, biológico, químico (NRBQ) para organizaciones y por organizaciones terroristas.

15 Blanco Navarro, J. M. (junio de 2013). Hacia una cultura de seguridad nacional. Documento nº 1 de Cultura de Seguridad del Centro de Análisis y Prospectiva de la Guardia Civil (pp. 12-13). Recuperado el 1 de julio de 2013, del sitio web: http://www.iuisi.es/20_fuentes_abiertas/001%20HACIA%20UNA%20CULTURA%20DE%20SEGURIDAD%20NACIONAL.pdf

16 España, Congreso de los Diputados. (31 de enero de 2012). Ob., cit. pp. 4-6.

España trabaja con otros organismos bilateralmente o multilateralmente en foros, principalmente de la UE, ONU y OSCE para promover y coordinar la lucha contra el terrorismo. Ésta última organización, presentó un informe[17] de abril de 2013, sobre las medidas para prevenir y combatir el terrorismo, aportando una lista de acuerdos y protocolos. En el marco de la Estrategia de Seguridad Interior de 2010 de la UE[18] (EU Internal Security Strategy ISS "in action"), uno de los cinco objetivos estratégicos, está relacionado con la prevención del terrorismo y la lucha contra la radicalización y el reclutamiento de terroristas. También España está comprometida con la participación en el Foro Global contra el Terrorismo (Global Counterterrorism Forum ,GCTF) y en el seno del Consejo de Seguridad de Naciones Unidas con el Comité contra el Terrorismo (Counter Terrorism Committee, CTC).

De la misma forma las relaciones bilaterales son de vital importancia, destacando la cooperación entre España y Francia o la ampliación de la colaboración con Estados Unidos, con la firma del Memorando de Entendimiento[19] entre sus Fiscales Generales, para realizar investigaciones conjuntas e intercambio de información. Por otra parte el Gobierno está adaptando la legislación nacional a las exigencias de la lucha contra terrorista, en medidas como la prevención del blanqueo de capitales y la financiación del terrorismo. España adoptó y desarrolló en 2012 la Estrategia Integral contra el Terrorismo Internacional y la Radicalización, coordinada por el Centro Nacional de Coordinación Antiterrorista (CNCA).

Siguiendo con este ámbito, el Secretario de Estado de Seguridad del Ministerio del Interior[20], destaca la lucha contra el Terrorismo en su "eje estratégico 1":

La amenaza que representa el terrorismo, fenómeno cada día más transnacional e interconectado, permite a España demostrar su compromiso con la seguridad global y la adopción de un enfoque proactivo en la cooperación policial internacional. Con la Estrategia integral contra el Terrorismo Internacional y la Radicalización de 2012, dirigida a neutralizar la amenaza que representa el terrorismo internacional y reducir la vulnerabilidad de la sociedad a sus ataques, haciendo frente a los procesos de radicalización que lo puedan preceder o sustentar. La Estrategia, que se desarrolla en 29 líneas de actuación, tiene un esquema basado en tres grandes líneas de acción: actuar en el origen y sobre las causas que generan la radicalización (PREVENIR); disminuir nuestras vulnerabilidades (PROTEGER); y hacer frente a la actividad terrorista (PERSEGUIR). La acción de las FCSE, en colaboración con países socios y amigos (en especial de Francia, el Reino Unido, Italia y Brasil), ha permitido que, desde el 22 de noviembre de 2011, hayan sido detenidos 59 miembros de ETA, 13 de miembros de la kale borroka, así como 5 integrantes de los GRAPO, 8 de Resistencia Galega y 21 miembros de grupos terroristas de carácter internacional (yihadismo y PKK).

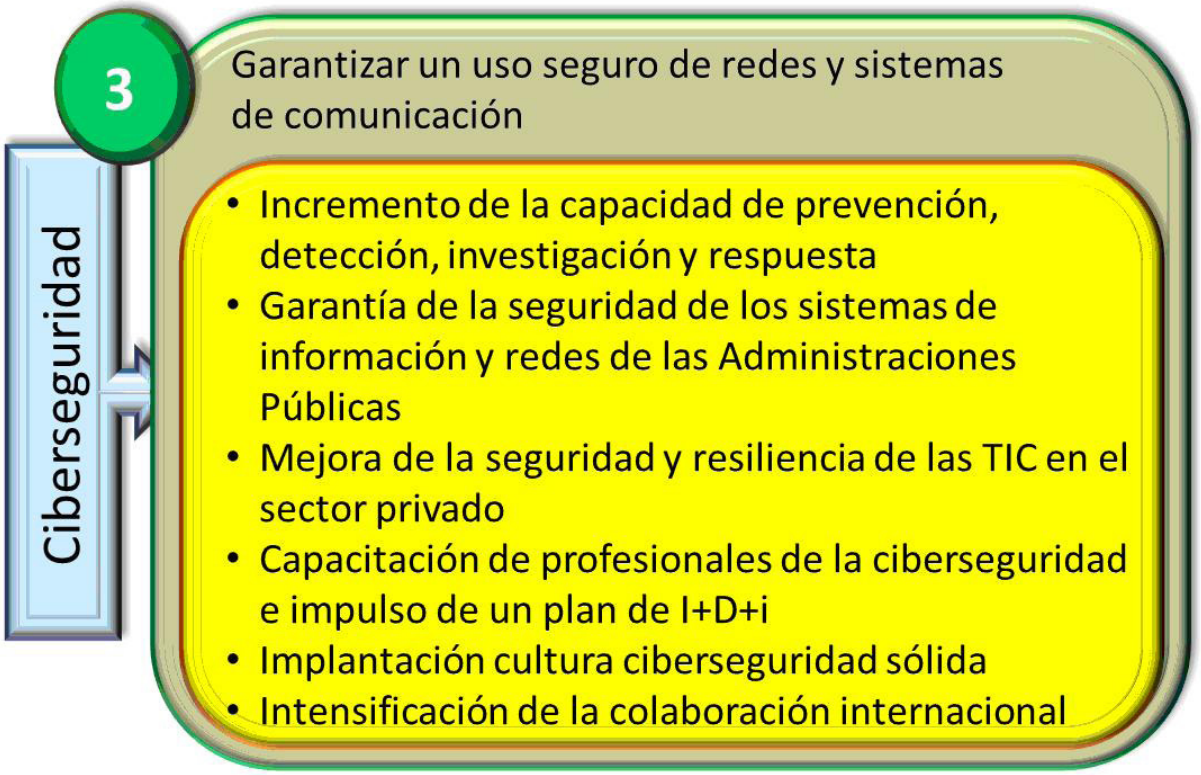
17 España, representante permanente ante la OSCE. (15 de abril de 2013). Nota verbal de la Representación Permanente, sobre información de aspectos Político-militares de la seguridad. FSC. EMI/62/13. Recuperado el 10 de agosto de 2013, del sitio web: http://www.osce.org/es/fsc/100719

18 European Union. (22 de noviembre de 2010). The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. COM(2010) 673 final. (pp. 7-9). Recuperado el 10 de junio de 2013, del sitio web: http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/news/internal_security_strategy_in_action_en.pdf

19 Estados Unidos, Embajada en Madrid. (10 de diciembre de 2013). Hoja informativa sobre cooperación entre España y Estados Unidos en el ámbito de seguridad. Recuperado el 18 de diciembre de 2013, del sitio web: http://photos.state.gov/libraries/spain/192041/pressreleases/13-1210_Fact_Sheetb_sp.pdf

20 España, Comisión de Interior del Consejo de los Diputados. (18 de junio de 2013). Ob. cit., pp. 3-5.

4. CIBERSEGURIDAD



Normalmente los ciberataques comparten unas características comunes[21], como el bajo coste, el fácil empleo, la efectividad y el bajo riesgo para el atacante. Los agentes que pueden realizar alguna acción en el ciberespacio son variados, desde los propios Estados, los grupos extremistas (ideológicos o políticos), el crimen organizado, o las actuaciones delictivas individuales. Por su impacto podría destacarse a las organizaciones delictivas relacionadas con el robo de tarjetas de crédito o certificados digitales, el fraude telemático, el blanqueo de dinero y el robo de identidades asociado a la inmigración ilegal. También el espionaje industrial y el Hawking político (como por ejemplo los ataques de denegación de servicio entre China y Japón, India y Pakistán o entre árabes e israelíes), los servicios de inteligencia o unidades cibernéticas de Fuerzas Armadas, manejan información sensible y pueden especializarse con recursos técnicos para actuar contra otros sistemas de seguridad, sobre todo éstas últimas en tiempo de crisis o conflictos. Por último, aparece el ciberterrorismo destacado por el uso de ciberataques con efectos catastróficos y pánico generalizado.

Todo lo anterior hace que el Gobierno español promueva líneas de acción concretas contra éste fenómeno, dando como resultado el nacimiento de la Estrategia de Ciberseguridad Nacional[22], aprobada por el Consejo de Seguridad Nacional el 5 de di-

21 Candau Romero, J. (2011). Estrategias nacionales de ciberseguridad. Ciberterrorismo. Cap. VI. En IEEE, Instituto Español de Estudios Estratégicos, Ciberseguridad. retos y amenazas a la seguridad nacional en el ciberespacio. Cuaderno de seguridad nº 149 (págs. 259-322). Madrid: Ministerio de Defensa.

22 España, Consejo de Seguridad Nacional. (5 de diciembre de 2013). Nota de prensa: Aprobada la Estrategia de Ciberseguridad Nacional de 2013. Recuperado el 10 de diciembre de 2013, del sitio web: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf

ciembre de 2013, que responde a la creciente necesidad de preservar la seguridad en el ciberespacio por su enorme repercusión en cuestiones que afectan a la seguridad nacional, a la competitividad de la economía, el progreso y la prosperidad de nuestra sociedad. A continuación veremos algunas de las acciones a nivel ministerial que han sido emprendidas este ámbito:

- Ministerio del Interior. El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), es el órgano que se encarga de impulsar, coordinar y supervisar las actividades que tiene encomendada la Secretaría de Estado de Seguridad en relación con las infraestructuras críticas. Ésta Secretaría y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información han suscrito un acuerdo en el que, entre otros aspectos, se sientan las bases para la colaboración del CNPIC y el Instituto Nacional de Tecnologías de la Comunicación (INTECO) en materia de respuesta a incidentes para las tecnologías de la información de las infraestructuras críticas ubicadas en España, convirtiendo al INTECO en una herramienta de apoyo al CNPIC en la gestión de incidentes de ciberseguridad. Ambas entidades han puesto en marcha los equipos para la respuesta a incidentes de seguridad (CERT) especializados en el análisis y gestión de problemas e incidencias de seguridad tecnológica, y el centro para la respuesta a incidentes en infraestructuras críticas (CERT-IC). Además el CNPIC colabora con el Centro Criptológico Nacional (CCN) y presenta una serie de guías de interés para la seguridad de los sistemas de control industrial, también conocidas como “SCADA”. También hay que citar, por su importancia destacada al grupo de delitos telemáticos de la Guardia Civil, a la Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía, Protección Civil, Aviación Civil, el Consejo de Seguridad Nuclear y las Policías Autonómicas que colaboran en éste área.

- Ministerio de Hacienda y AAPP. El 15 de enero de 2013, el ministro Cristobal Montoro, presidió el Consejo Superior de Administración Electrónica, donde se aprobaron las líneas estratégicas del plan de Administración Electrónica del Gobierno 2013-2015.

- Ministerio de Industria, Energía y Turismo. La Secretaría de Estado de Telecomunicaciones y Sociedad de la Información, desarrolla el empleo de las tecnologías de la información con el “Plan Avanza[23]”. La industria de la ciberseguridad ha experimentado en los últimos años un notable crecimiento derivado del incremento en la cantidad y en la magnitud de los incidentes de seguridad sucedidos. Esta tendencia se presenta asimismo como una oportunidad para la iniciativa privada de desarrollar una industria capaz de satisfacer la cada vez mayor demanda de soluciones de ciberseguridad. Con estos avances realizados en los años anteriores, hacen previsible el cumplimiento de los objetivos en materia de seguridad planteados por la Agenda Digital para Europa[24].

23 Vid. Consejo de Ministros de 16 de julio de 2010, donde se acordó la Estrategia 2011-2015 del Plan Avanza.

24 España, Ministerio de Industria, Energía y Turismo. (22 de junio de 2012). Informe de recomendaciones del Grupo de expertos de Alto Nivel de la Agenda Digital para España. (pp. 51-52). Recuperado el 17 de agosto de 2013, del sitio web: http://www.minetur.gob.es/telecomunicaciones/es-es/novedades/documents/informe-recomendaciones-ade.pdf

- CNI. Adscrito al Ministerio de la Presidencia (según su nuevo estatus regulador, BOE nº 89, de 13 de abril de 2013), es un organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión, incluidas las ciberamenazas. Cuenta con la Oficina Nacional de Seguridad (ONS) para la protección de la información clasificada y el CCN (RD 421/2004) para la seguridad de los sistemas de las tecnologías de la información de la Administración. Dentro del CCN se encuentran integrados los Computer Emergency Response Team (CERT) equipos de respuesta a incidentes de seguridad de la información, que trabajan en la seguridad de los sistemas y en evitar o minimizar los ataques que se produzcan contra estos.
- Ministerio de Defensa. Dispone de una política de seguridad con responsabilidades sobre sistemas que manejan información clasificada, distribuidas entre la Dirección General de Infraestructuras, el Estado Mayor de la Defensa (EMAD) y los Cuarteles Generales de los tres Ejércitos. El Jefe del EMAD, tiene bajo su dirección el Mando Conjunto de Ciberdefensa. También encuadrado en la Subdirección General de Tecnologías de la Información y Comunicaciones trabaja el Centro[25] de Operaciones de Seguridad de la Información del Ministerio de Defensa (COSDEF). En enero de 2011 el JEMAD elaboró el documento[26] "Visión de la Ciberdefensa Militar", en el cual se incluye al ciberespacio como uno de los dominios de enfrentamiento, siendo los otros tierra, mar, aire y el espacio exterior. Después, en julio de 2011 el JEMAD apruebó el "Concepto de la Ciberdefensa Militar" (CDM) en el que se establecen los principios, objetivos y retos de la ciberdefensa en el ámbito militar, define la terminología, realiza una valoración de la capacidad, y ordena la elaboración de un Plan de Acción de Ciberdefensa Militar.

En el contexto internacional, las Naciones Unidas, publicaron en marzo de 2013, un documento/índice[27] se seguridad Internacional de amenazas y realidad actual. Poco después el 4 de mayo, aparece el Centro de Ciberseguridad Industrial, que aspira a convertirse en el punto independiente de encuentro entre los organismos privados y públicos, relacionados con las prácticas y tecnologías aplicadas a la ciberseguridad industrial. También la UE, un mes después de poner en marcha el Centro Europeo de Ciberdelincuencia (European Cybercrime Centre, EC3), publicó en febrero de 2013, su Estrategia de Ciberseguridad[28] "un espacio abierto, protegido y seguro".

Con respecto a las líneas de acción del Ministerio del Interior, el Secretario de Estado de Seguridad[29], incide en la actuación de las FCSE en su "eje estratégico 2":

25 Vid. BOD nº 251, de 28 de diciembre de 2011 (pp. 33507-33510). Instrucción 96/2011 del Secretario de Estado de Defensa por la que se crea el COSDEF).

26 Zea Pasquín, F. (6 de marzo de 2013). Ciberdefensa Militar. Revista española de Defensa, nº 293. (pp. 48-49). Recuperado el 11 de mayo de 2013, del sitio web: http://www.defensa.gob.es/Galerias/documentacion/revistas/2013/red-293-ciberdefensa.pdf

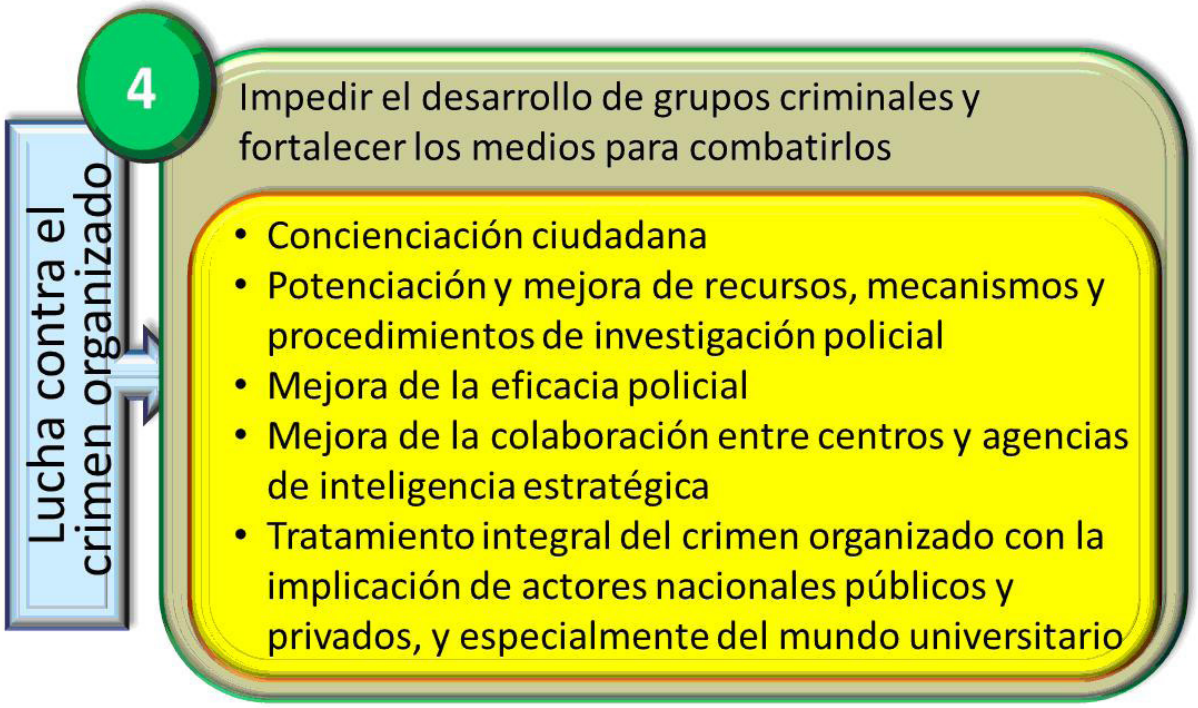
27 United Nations. (marzo de 2013). The Cyber index. International security trends and realities. UNIDIR United Nations Institute for Disarmament Research. Recuperado el 2 de agosto de 2013, del sitio web: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

28 European Union. (7 de febrero de 2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN (2013) 1 final. Recuperado el 17 de agosto de 2013, del sitio web: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

29 España, Comisión de Interior del Consejo de los Diputados. (18 de junio de 2013). Ob., cit., pp.

El desafío de la ciberdelincuencia, un nuevo reto que requiere y, a la vez, impulsa la modernización de nuestras fuerzas policiales, así como la necesidad de colaborar con las instituciones privadas que operan las infraestructuras críticas y las redes de comunicación, por ejemplo: utilización por menores (además de la pornografía infantil, se dan casos de grooming o acoso sexual, ciberbulling o acoso vejación, captación de menores por pederastas en las redes sociales o publicación incontrolada de datos personales); delincuencia organizada (robo de datos bancarios o datos personales, desbloqueo de malware, etc.); Hacktivismo (ataques de denegación de servicio de índole económico o reivindicativo); espionaje industrial (puede suponer la quiebra total de una empresa); y ciberterrorismo (usando Internet como instrumento de comunicación o de ataque a infraestructuras críticas u objetivos estratégicos). Se crea la Oficina de Coordinación Cibernética, en el seno del CNPIC.

5. LUCHA CONTRA EL CRIMEN ORGANIZADO



La lucha contra el crimen organizado está presente en la preocupación política del Ministerio del Interior y en el día a día de las FCSE. Si analizamos los últimos documentos del Ministerio del Interior, reflejan que la lucha contra esta amenaza es integral. Por ejemplo, el 2 de noviembre de 2010, el ministro del Interior comparece ante la Comisión de Interior para informar sobre el balance de la lucha contra el crimen organizado en España en el año anterior, relatando los aspectos definitorios sobre el Crimen Organizado en España, la situación actual y la respuesta estratégica. Así explicó entre otros datos de interés: la modificación del Código Penal con la aplicación de la LO 5/2010, de 22 de junio, que modifica el concepto de organización criminal; el trabajo desempeñado por el Centro de Inteligencia contra el Crimen Organizado (CICO), creado 2006 que elabora la inteligencia estratégica y los criterios de coordinación operativa[30].

7-10.

30 España, Ministerio del Interior. (2 de noviembre de 2010). Comparecencia lucha contra el Crimen Organizado. Recuperado el 24 de agosto de 2013, del sitio web: http://www.interior.gob.es/file/11/11187/11187.pdf

Así en 2010, los ejes de la respuesta estratégica contra el crimen organizado eran los siguientes:

- Más y mejor inteligencia e incremento de recursos policiales.
- Organización especializada. Actuación especializada de la Guardia Civil con su Grupo de Delitos Telemáticos de la Guardia Civil (GDT), Equipos de Investigación Tecnológica (EDITE), Grupos de Apoyo en Tecnología de la Información (GATI) y Equipos de investigación contra el Crimen Organizado (ECO). Por parte del Cuerpo Nacional de Policía, las Brigadas de investigación tecnológica y los Grupos de respuesta especializada contra el crimen organizado.
- Cooperación y coordinación internacional (Comité de Seguridad Interior) con Agencias, Instituciones y Organismos de la UE (EUROPOL, EUROJUST y FRONTEX). Refuerzo de Consejeros y Agregados en embajadas españolas, colaboración con INTERPOL. Mejora de la información y cooperación con los países de la Comunidad de Estados Independientes y cooperación bilateral con países de África Occidental y del Golfo de Guinea.
- Perfeccionamiento legislativo. Modificación Código Penal, Ley de Enjuiciamiento Criminal y Ley de Represión del Contrabando. Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo.

En 2011, el Ministerio del Interior elaboró la estrategia española 2011-2014, contra el crimen organizado con seis ejes prioritarios[31]:

1. Potenciar la inteligencia contra el crimen organizado. Reforzar el CICO y las unidades de inteligencia de Guardia Civil y Policía.
2. Atacar a la economía del crimen organizado. Con los objetivos de identificación de propietarios de empresas y fondos, acceso a los registros de cuentas bancarias y eficacia en la incautación y gestión de activos interceptados.
3. Atacar las actividades de narcotráfico, corrupción, blanqueo de capitales, cibercrimen, tráfico, trata y explotación de seres humanos, delitos contra la propiedad intelectual e industrial, y fraude del IVA, falsificación del euro y de documentos.
4. Reforzar las capacidades operativas de Guardia Civil y Policía con el incremento de especialización y recursos materiales y humanos.
5. Impulsar la coordinación y cooperación internacional: Desarrollo de los planes de acción en la UE (EUROPOL, EUROJUST, OLAF y estados miembros) e impulso de una Fiscalía Europea contra el Crimen Organizado.
6. Fomentar la participación del sector público y privado afectado.

También el balance[32] de 2012 realizado por el Ministerio del Interior sobre el Crimen

31 España, Ministerio del Interior. (1 de septiembre de 2011). Lucha contra el crimen organizado. Balance 2010 y estrategia española 2011-2014. Recuperado el 17 de agosto de 2013, del sitio web: http://www.interior.gob.es/file/52/52412/52412.pdf

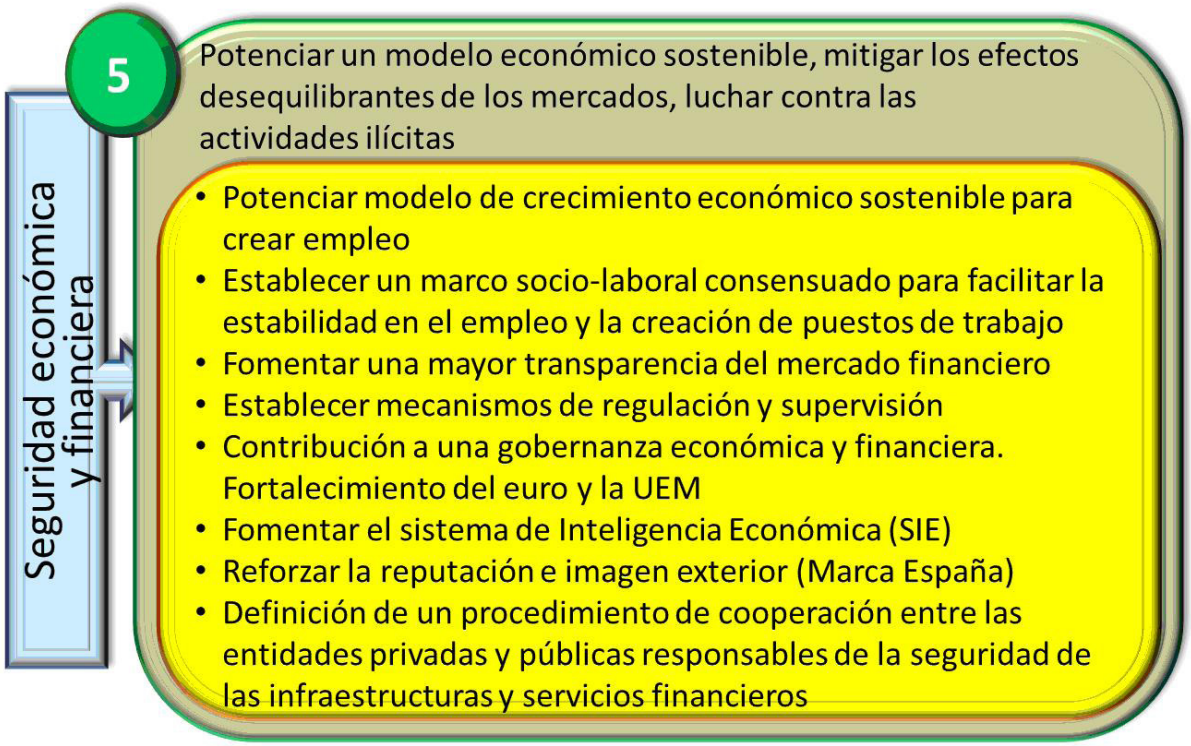
32 España, Ministerio del Interior. (1 de julio de 2013). Lucha contra el crimen organizado. Balance 2012 y avance enero mayo 2013. Recuperado el 31 de agosto de 2013, del sitio web: http://www.interior.gob.es/file/62/62590/62590.pdf

Organizado, explica los criterios de la denominación de "grupo de crimen organizado", según las normas de EUROPOL y diferencia entre grupos de alta intensidad, grupos típicos y grupos de baja intensidad. Los grupos totalmente desarticulados en 2012 fueron de 277 y otros 172 fueron parcialmente desarticulados. Las principales actividades de los grupos de crimen organizado se centraron en: el tráfico de cocaína y hachís; estafa; robo con fuerza, robo de vehículos, armas, ordenadores, telefonía móvil; y falsificación de euros.

Por último, en este ámbito, las líneas de acción de la Secretaría de Estado de Seguridad del Ministerio del Interior, se observan en su "eje estratégico 1", relacionado con el crimen organizado[33]:

La Estrategia Española de Lucha contra el Crimen Organizado de 2011-2014 (coordinada por el CICO), pone de relieve la diversidad de delitos de las organizaciones criminales: narcotráfico, corrupción, blanqueo de capitales, cibercrimen, tráfico y explotación de seres humanos (la Guardia Civil como el CNP tienen en vigor y actualizan constantemente planes operativos contra la Trata de Seres Humanos con fines de Explotación Sexual), robo de propiedad intelectual, fraude impositivo y falsificación. Pero también resalta esta Estrategia que no son delitos aislados, sino que las mismas redes, los mismos canales de transporte, las mismas operaciones de lavado de capitales y la misma financiación opaca sirven a un complejo delictual íntimamente entrelazado.

6. SEGURIDAD ECONÓMICA Y FINANCIERA



La necesidad de conocer acciones hostiles dirigidas contra los intereses geoeconómicos de España y anticipar el movimiento de indicadores económicos clave en un entorno de información incompleta se convierte en una necesidad vital para la toma de decisiones, por lo que es necesario incrementar las capacidades

33 España, Comisión de Interior del Consejo de los Diputados. (18 de junio de 2013). Ob. cit., pp. 5-7

de inteligencia económica del Estado. La seguridad económica por tanto, es un fin amplio buscado por todos los Gobiernos[34].

En este ámbito la UE busca políticas de cohesión que se orienten en la mejora y la posición competitiva del conjunto de la UE y de sus regiones, en particular las menos desarrolladas, a través del Fondo Europeo de Desarrollo Regional (FEDER), el Fondo Social Europeo y el Fondo de Cohesión. La Comisión de la UE, plantea cambios importantes en la política de cohesión, en aras a contribuir a la consecución de los objetivos y metas en materia de crecimiento y empleo de la Estrategia Europa 2020. Así la política de cohesión para el periodo 2014-2020[35], recoge la existencia de un Acuerdo de Asociación entre el Estado miembro y las instituciones comunitarias para la programación de los Fondos del Marco Estratégico Común, En este informe se recogen los objetivos de la "futura política de cohesión", que están en conexión con la Estrategia Española de Política Económica, y con los datos del Balance y Actualización (2013)[36], mencionando que España ha logrado acelerar la reducción del déficit público y converger con el resto de Europa, forjando las bases para la recuperación del crecimiento y la creación de empleo.

Pasando a otra línea de acción de este ámbito, el Consejo de Ministros de 28 de junio de 2013, aprobó el primer Plan Anual de Acción Exterior de la Marca España, con el objetivo que para 2014 se presente un plan integrador que incida en las sinergias que se puedan suscitar entre todos los actores implicados y en el que la Marca España pueda desarrollar su labor de coordinación. En este sentido es esencial la colaboración público privada (CPP) entre la administración y empresas privadas, por ejemplo en la gestión de servicios, infraestructuras y otros acuerdos como las peculiaridades de las industrias de seguridad de la defensa.

Con respecto a la racionalización del gasto, hace que se incremente la competitividad y la colaboración con entidades de otros países y redes internacionales para compartir la investigación y desarrollo tecnológico, por ejemplo, con la participación en los proyectos del 7º Programa Marco de la UE, que finalizaron en 2013 dando paso a "Horizonte 2020". En este sentido el Ministerio del Interior creó el Grupo de Investigación e Innovación en Seguridad que sirve de apoyo para las empresas que planteen iniciativas en el tema de I+D+i, relacionadas con la investigación relativa a tecnologías y conocimientos de seguridad (seguridad ciudadana; seguridad de infraestructuras y servicios; vigilancia inteligente y seguridad fronteriza; y restablecimiento de la seguridad en caso de crisis)[37]. Por otra parte, la Guardia Civil con el desarrollo del programa COOPERA ha puesto de manifiesto la importancia que para la seguridad pública tiene

34 Ferrer Rodríguez, J. (5 de diciembre de 2011). Seguridad económica inteligencia estratégica de España. Documento de Opinión nº 85. (pp. 4-5). Recuperado el 10 de agosto de 2013, del sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO85-2011SeguridadEconomicaIntEstEspana_JFerrer.pdf

35 España, Consejo Económico y Social. (23 de enero de 2013). Informe Consejo Económico y Social. El acuerdo de asociación de España en el marco de la política de cohesión 2014-2020. Recuperado el 14 de septiembre de 2013, del sitio web: http://www.ces.es/documents/10180/526241/Inf0213.pdf

36 España, Presidencia del Gobierno. (26 de abril de 2013). Balance y Actualización de la Estrategia Española de Política Económica, programa nacional de reformas. Recuperado el 7 de septiembre de 2013, del sitio web: http://www.lamoncloa.gob.es/NR/rdonlyres/3D6CF215-0DC1-4DAD-8688-A4E59B27B6BB/0/130423_BALANCE_PNR_30_PRENSA.pdf

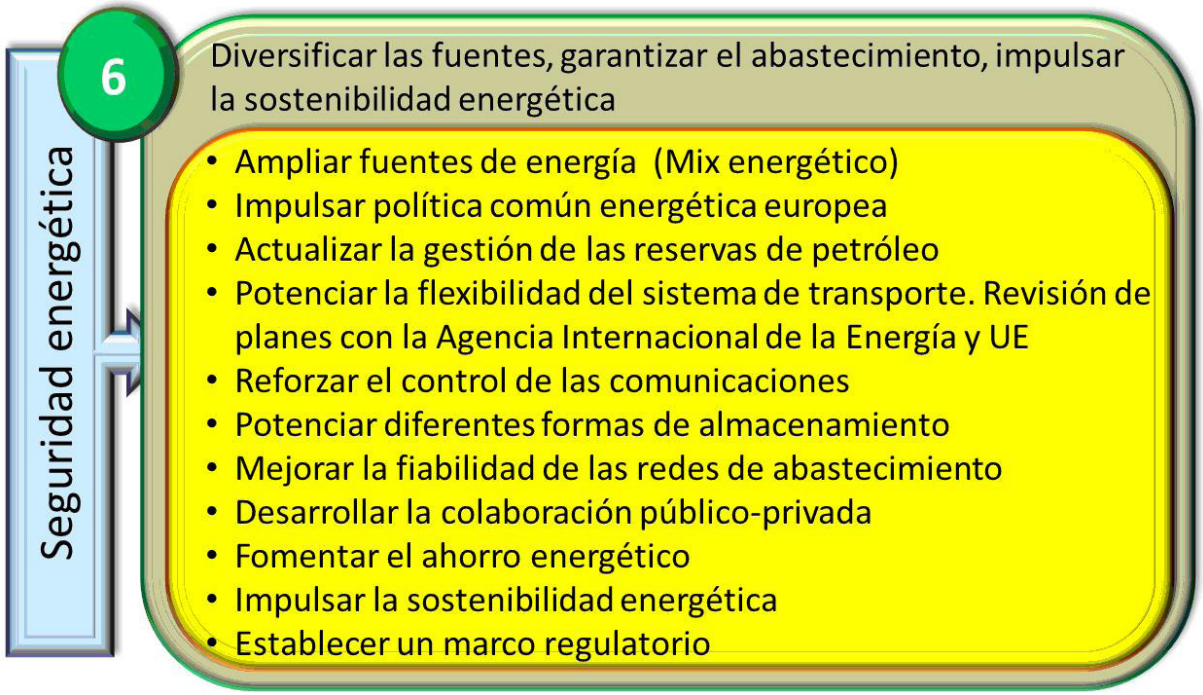
37 Acuerdo del CMU, por el que se crea el 7 de octubre de 2009 el Grupo Técnico Permanente sobre I+D+i en Seguridad (GISEC), constituido el 23 de enero de 2010.

la colaboración con empresas de seguridad. De esta forma, el 14 de noviembre de 2013, la Guardia Civil puso en marcha el programa "Plus Ultra" con el que pretende mejorar la seguridad de las empresas españolas que se establezcan o lleven a cabo proyectos de negocio en el extranjero[38].

A continuación vemos el "eje estratégico 8", de las líneas de acción de la Secretaría de Estado de Seguridad del Ministerio del Interior[39]:

Esfuerzo de eficiencia y racionalización del gasto, apostando por la modernización de los sistemas de información, bases de datos y sistemas de comunicación, desarrollando nuevos proyectos destacando: Proyecto de "Fronteras Inteligentes" con el Centro Nacional de Gestión y coordinación de Fronteras, el proyecto de localización de vehículos robados en tiempo real, el desarrollo del nuevo sistema de radiocomunicaciones digitales de emergencia del Estado, SIRDEE, y la puesta en funcionamiento del denominado SIMASC (Sistema de Movilidad de Alertas de Seguridad Ciudadana) a través de una aplicación móvil.

7. SEGURIDAD ENERGÉTICA



La nueva concepción de la Seguridad Energética en la doctrina de la OTAN parte de su Concepto Estratégico de 2010, seguido de la reorganización de la Emerging Security Challenges Division (ESCD) y la creación del Centro de Excelencia OTAN de Seguridad Energética en Lituania (2012)[40]. En España la Ley 8/2011, de protección de infraestructuras críticas y el CNPIC se centran en el concepto de la seguridad física relacionado con las instalaciones y redes de energía, y en la Estrategia de Seguridad Nacional (ESN-2013), aparece en el nuevo contexto geoestratégico la vulnerabilidad energética, acrecentada en la actualidad por el incremento de la demanda de energía, siendo ésta un factor clave para el progreso económico.

38 España, Guardia Civil. (14 de noviembre de 2013). Programa Plus Ultra de la Guardia Civil. Recuperado el 20 de noviembre de 2013, del sitio web: http://www.guardiacivil.es/documentos/seprose/formularios/programa_plus_ultra.pdf

39 España, Comisión de Interior del Consejo de los Diputados. (18 de junio de 2013). Ob. cit., pp. 14-15.

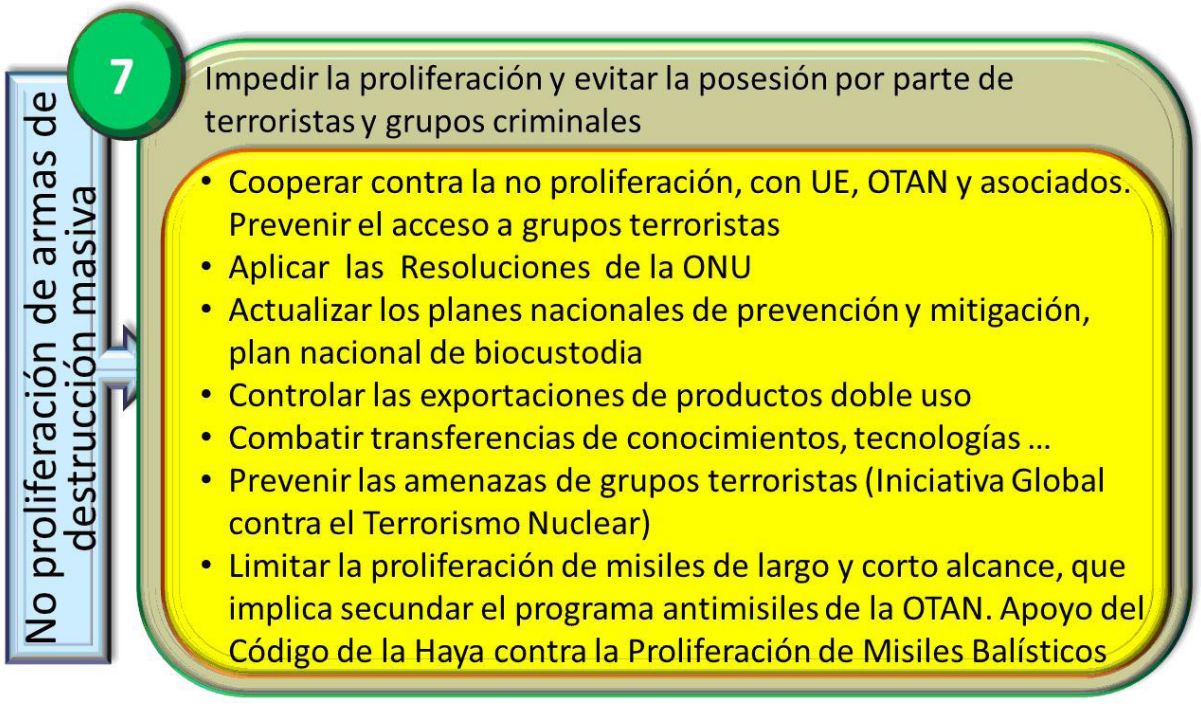
40 De Espona y Rodríguez, R. J. (2 de abril de 2013). Ob. cit., pp. 3-5.

El Ministerio del Interior es consciente de todo lo anterior y considera vital garantizar la seguridad de las fuentes de energía para el desarrollo económico del país[41] y de la misma forma, el Secretario de Estado de Seguridad, asegura que la coordinación de los organismos públicos y la estrecha colaboración de los operadores privados es necesaria para prevenir la amenaza terrorista contra las infraestructuras de energía[42]. Así la seguridad energética depende de distintos factores, desde la oferta adecuada de precios asumibles, la seguridad de las instalaciones y redes de transporte, hasta la sostenibilidad ambiental, los ataques intencionados o desastres naturales.

De esta forma los Estados desarrollan su política energética de maneras diversas, según el predominio del modelo de sector público o privado y la presencia de organizaciones internacionales del sector energético en general, como la Agencia Internacional de la Energía, "International Energy Agency IEA", o de un sector concreto como la Organización de Países Exportadores de Petróleo "Organization of the Petroleum Exporting Countries OPEC" o la Agencia Internacional de la Energía Atómica "International Atomic Energy Agency IAEA".

La IEA, aprobó una nueva estrategia global en 2012, que sienta las bases para la participación práctica e institucional con los países socios, y en su informe ejecutivo establece su "visión de las cuatro E": energy security (and markets), la seguridad energética (y mercados); Environmental sustainability (and technology), la sostenibilidad ambiental (y tecnología); Economic development (and forecasting), el desarrollo económico (y previsión); y Engagement globally, compromiso global[43].

8. NO PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA



41 España, Congreso de los Diputados. (31 de enero de 2012). Ob., cit. p. 4.
42 España, Comisión de Interior del Consejo de los Diputados. (18 de junio de 2013). Ob., cit., p. 9.
43 International Energy Agency. (1 de marzo de 2013). 2012 annual report. (pp. 4-5). Recuperado el 7 de septiembre de 2013, del sitio web: http://www.iea.org/publications/freepublications/publication/IEA_Annual_Report_publicversion.pdf

En este ámbito de actuación, el Ministerio del Interior apoya las medidas que está tomando la comunidad internacional en el control de la proliferación de armas de destrucción masiva (ADM), dado los riesgos evidentes que podría ocasionar su uso, para la estabilidad internacional, teniendo en cuenta que las zonas de mayor proliferación de este tipo de armas coinciden con aquellas áreas con una frágil estabilidad política e institucional. Entre los artículos de fabricación nacional que mayor preocupación pudieran conllevar desde el punto de vista de la proliferación de ADM se encuentran los de las industrias aeronáuticas y espaciales, susceptibles de ser desviados a programas de misiles, así como los aviones aéreos no tripulados (UAS), de gran proyección actualmente y que pueden ser utilizados como medios de lanzamiento por sí mismos. También exigen una especial atención las máquinas y herramientas de gran empleo en todo tipo de programas sensibles y que son utilizadas para múltiples tareas industriales, desde la fabricación del cono de un misil balístico hasta la mecanización de un tapón de tungsteno para un artefacto nuclear de tipo pistola, todo ello sin contar con el gran número de válvulas, tubos, aluminios, etcétera, de fabricación nacional que pudieran ser mal empleados para la fabricación de centrifugadoras de enriquecimiento de uranio, intercambiadores de calor de industrias nucleares o columnas de destilación para ámbitos químicos, por mencionar algunos ejemplos, ámbito en el que la cooperación las Fuerzas y Cuerpos de Seguridad con otros cuerpos policiales es intenso, exigiendo una permanente acción preventiva[44].

Siguiendo con este ámbito, sobre la línea de acción que trata de la cooperación entre países para evitar y prevenir la adquisición por terroristas de ADM, sus vectores y los materiales y tecnologías relacionados con su fabricación, es un tema que está en la agenda de las Naciones Unidas, por ejemplo el informe de la Asamblea general de agosto de 2003, en el que hace constar las medidas sobre que han realizado varios países para evitar que este tipo de armas lleguen a manos de grupos terroristas[45]. También la UE en 2003, acordó su Estrategia[46] contra la proliferación de ADM, subrayando la importancia de actuar con determinación para prevenir, disuadir, detener y eliminar los programas de proliferación de ADM y misiles, y en 2006 el Consejo aprobó un documento conceptual del seguimiento y mejora de la aplicación coherente de la estrategia de la UE contra la proliferación de las ADM, publicando en 2013 publica los progresos de su implantación[47].

La base jurídica para todos los esfuerzos que están realizando los Estados, se encuentran en las normas establecidas en los tratados internacionales y sus protocolos, por ejemplo: el Tratado sobre la no proliferación de las armas nucleares, los acuerdos con el Organismo Internacional de Energía Atómica (International Atomic Energy

44 España, Comisión de Interior del Consejo de los Diputados. (18 de junio de 2013). Ob. cit., pp. 11-13.

45 United Nations. (1 de agosto de 2003). Medidas para evitar la adquisición por terroristas de armas de destrucción en masa. A/58/208. Recuperado el 7 de septiembre de 2013, del sitio web: http://www.cinu.org.mx/multi/ter/documentos/ares58_208.pdf

46 European Union. (10 de diciembre de 2003). Fight against the proliferation of weapons of mass destruction. EU strategy against proliferation of Weapons of Mass Destruction. PESC 768. Recuperado el 7 de septiembre de 2013, del sitio web: http://register.consilium.europa.eu/pdf/en/03/st15/st15708.en03.pdf

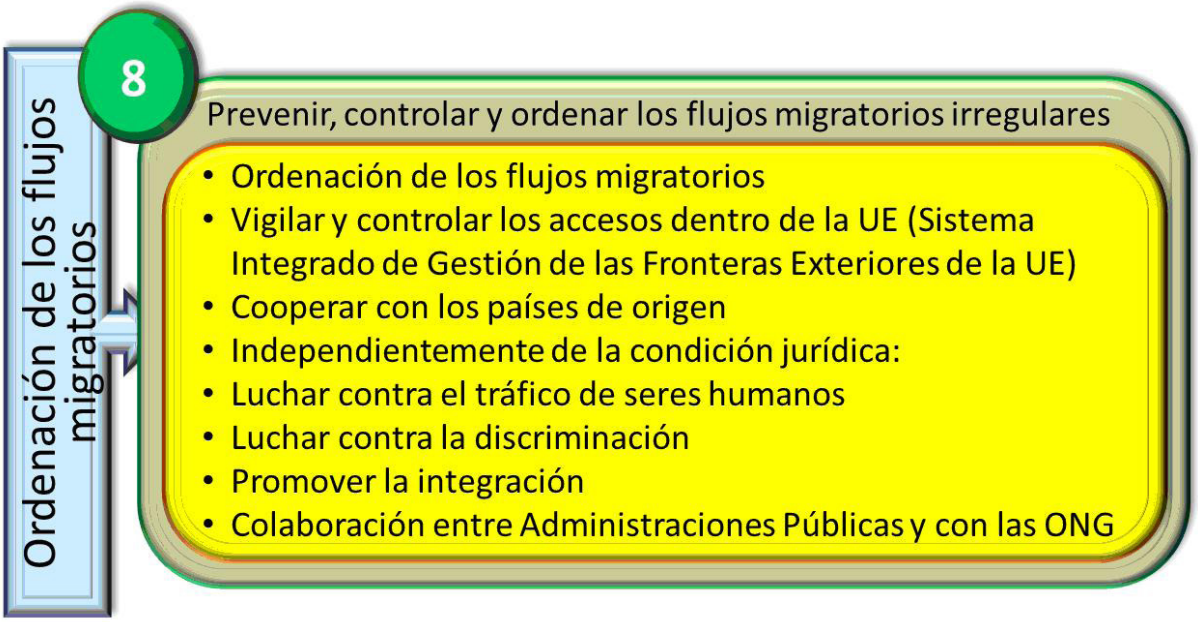
47 European Union. (9 de febrero de 2013). Six-monthly Progress Report on the implementation of the EU Strategy against the Proliferation of Weapons of Mass Destruction. Official Journal of the EU 2013/C 37/0. Recuperado el 14 de septiembre de 2013, del sitio web: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:037:0003:0026:EN:PDF

Authority, OIEA), la Convención sobre armas químicas (CWC), la Convención sobre las armas biológicas y toxínicas (Biological and Toxin Weapons Convention, BTWC), el Código internacional de conducta contra la proliferación de misiles balísticos y la comisión del Tratado de prohibición de los ensayos nucleares. Además la estrecha colaboración con socios como Estados Unidos, Rusia, Japón y Canadá, las Naciones Unidas y otras organizaciones internacionales, son esenciales para la aplicación efectiva del régimen de no proliferación de ADM.

En este ámbito también se hace referencia a la "biocustodia", siendo una línea de acción que obliga actualizar los planes nacionales de prevención y mitigación de los riesgos en los ámbitos nucleares, bacteriológicos y químicos, recordando las consideraciones realizadas en la Convención sobre la prohibición y el almacenamiento de armas bacteriológicas (biológicas) y toxínicas, sobre su destrucción[48].

Para finalizar este ámbito tan solo recordar la reunión interprofesional del Grupo de Aplicación y Evaluación de la Iniciativa Global contra el Terrorismo Nuclear (IGTN), que fue realizada en febrero de 2013 en Madrid, en la que participaron expertos de 61 países y de organizaciones como la UE, las Naciones Unidas, el Organismo Internacional de la Energía Atómica y la INTERPOL[49].

9. ORDENACIÓN DE FLUJOS MIGRATORIOS



En relación a la gestión de fronteras, su vigilancia y control de los accesos dentro

48 United Nations. (31 de octubre de 2008). Medidas nacionales, regionales e internacionales para mejorar la bioseguridad y la biocustodia, en particular la seguridad en el laboratorio y la seguridad de los patógenos y toxinas. BWC/MSP/2008/L.1. Recuperado el 14 de septiembre de 2013, del sitio web: http://www.opbw.org/new_process/msp2008/BWC_MSP_2008_L1_S.pdf

49 España, Presidencia del Gobierno. (22 de febrero de 2013). Finaliza en Madrid la reunión anual de la iniciativa global contra el terrorismo nuclear (IGTN). Recuperado el 14 de septiembre de 2013, del sitio web: http://www.lamoncloa.gob.es/ServiciosdePrensa/NotasPrensa/MAE/2013/220213IniciTerrorismNuclear.htm

de la UE, han sido muchos los avances, centrados en el artículo 77 de Tratado[50] de Funcionamiento de la UE (TFUE), antiguo artículo 62 del Tratado constitutivo de la Comunidad Europea, (TCE). Se trata de que a la vez que se garantiza la ausencia total de controles de las personas cuando crucen las fronteras interiores, la Unión establezca normas comunes respecto a los controles realizados en el cruce de las fronteras exteriores e instaure un sistema integrado para la gestión de dichas fronteras.

El primer paso hacia la gestión común de las fronteras exteriores de la Unión se dio el 14 de junio de 1985, cuando cinco de los entonces diez Estados miembros de la Comunidad Europea firmaron el Acuerdo de Schengen, complementado después por el Convenio de aplicación, las normas adoptadas conforme a esos textos y los tratados relacionados (acervo de Schengen). El espacio Schengen, formado actualmente por veintiséis países europeos, es el área sin fronteras creada por los tratados y acuerdos mencionados. Estas normas pueden dividirse en cinco categorías[51]:

1. Código de fronteras Schengen, que regula la circulación de personas por las fronteras Schengen.
2. Establecimiento de un cierto reparto de la carga financiera mediante el "Fondo Europeo para las Fronteras Exteriores (FEFE)".
3. Establecimiento de bases de datos centralizadas con vistas a la gestión de las fronteras y la migración: "Sistema de Información de Schengen (SIS)", el "Sistema de Información de Visados (VIS)" y el sistema EURODAC (base de datos europea de impresiones dactilares para identificar a los solicitantes de asilo y a los inmigrantes ilegales). Está a cargo de la nueva "Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud".
4. Medidas que eviten y sancionen la entrada, la circulación y la estancia irregular.
5. Medidas institucionales para la coordinación de la cooperación operativa en la gestión de las fronteras exteriores realizada por la "Agencia Europea para la gestión de la cooperación operativa en las fronteras exteriores de los Estados miembros de la UE (FRONTEX)".

El Ministerio del Interior realizó los primeros pasos hacia la gestión integrada de las fronteras exteriores, fortalecida en los últimos años con la infraestructura tecnológica, varias operaciones conjuntas contra la inmigración ilegal, y proyectos para un mayor control de inmigración irregular como por ejemplo: la puesta en marcha del "Sistema Integrado de Vigilancia Exterior" (SIVE) gestionado por la Guardia Civil en apoyo a sus funciones de vigilancia de la frontera sur; el proyecto comunitario EUROSUR (Sistema Europeo de vigilancia de las Fronteras); el desarrollo del plan piloto Fronteras Inteligentes; una activa política de repatriaciones y acuerdos de readmisión; el refuerzo de la cooperación bilateral; el proyecto de retorno voluntario de inmigrantes irregulares subsaharianos de la Organización Internacional para las Migraciones (OIM); los planes policiales contra la Trata de seres humanos con fines de explotación sexual o laboral y los nuevos mecanismos para la protección de los menores extranjeros no acompañados.

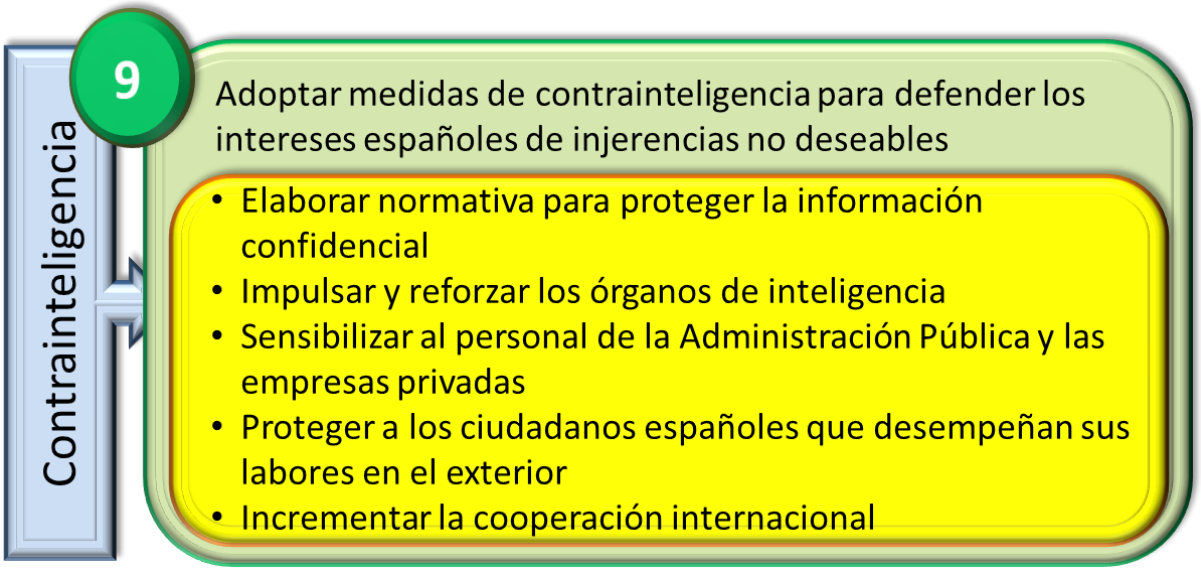
50 Vid. DOUE C 326/47-199, de 26 de octubre de 2012.

51 European Union. (1 de abril de 2013). La gestión de las fronteras exteriores. Ficha técnica Parlamento Europeo/Think Tank. Recuperado el 15 de septiembre de 2013, del sitio web: http://www.europarl.europa.eu/RegData/etudes/fiches_techniques/2012/041204/04A_FT%282012%29041204_ES.pdf

También el Ministerio del Interior apoyó la designación del Centro de Coordinación para la Vigilancia Marítima de Costas y Fronteras (CECORVIGMAR) en la sede de la Dirección General de la Guardia Civil, designado por FRONTEX como punto de contacto nacional de la red de vigilancia en el marco del proyecto EUROSUR. Este Centro está interconectado con los cuatro centros regionales de Valencia, Algeciras, Las Palmas, La Coruña y a las estaciones del SIVE, así como al nuevo sistema europeo de vigilancia de fronteras[52].

Por último destacar que el Consejo de la UE creó en 2007, los equipos de intervención rápida en las fronteras (RABIT) y un registro central de equipo técnico disponible (CRATE) para ayudar a los Estados miembros en caso de situaciones excepcionales y urgentes. Además la Comisión presentó en octubre de 2011 una propuesta sobre "fronteras inteligentes" y en febrero de 2013 otras relativas al "Sistema de Registro de Entradas y Salidas (SRES)" y el "Programa de Registro de Pasajeros (PRP)".

10. CONTRAINTELIGENCIA



En este ámbito, los organismos dedicados a labores e información e inteligencia en España, se pueden agrupar de forma generica en tres bloques: La inteligencia exterior, la militar y la interior.

La inteligencia exterior: La Ley[53] 11/2002, que regula el CNI, inspirada en los sistemas de los países de nuestro entorno, pretende organizar los servicios de la "comunidad de inteligencia" en una agencia central que le corresponde dirigir y coordinar. Su Director tiene que "desempeñar las funciones de Autoridad Nacional de Inteligencia y Contrainteligencia y la dirección del Centro Criptológico Nacional" (art. 9. 2,f). Luego

52 España, Ministerio del Interior. (16 de octubre de 2013). Inauguración del Centro de Coordinación para la vigilancia Marítima de Costas y Fronteras (CERCORVIGMAR). Recuperado del sitio web: http://www.interior.gob.es/press/jorge-fernandez-diaz-ensalza-la-gran-experiencia-de-espana-en-la-lucha-contra-la-inmigracion-irregular-que-la-situa-a-la-vanguardia-de-la-union-europea-15858?set_locale=gl

53 Vid. BOE nº 109, pp. 16440-16444. Reguladora del Centro Nacional de Inteligencia.

con el RD[54] 199/2012, el CN se adscribe al Ministerio de la Presidencia. También tiene como función la de velar por el cumplimiento de la normativa relativa a la protección de la "Información Clasificada", nacional e internacional. La propiedad de la información, su clasificación, custodia y acceso son algunos conceptos que se puede consultar[55] en la NS/04 "Seguridad de la Información" de la Autoridad Nacional para la protección de la información clasificada.

La inteligencia militar: El Ministerio de Defensa aprobó la Política de Seguridad de la Información, recogida en la Orden Ministerial[56] 76/2006. Esta norma define una estructura funcional de responsabilidades en la protección de la información. La política señala además los tres pilares básicos sobre los que se debe sustentar la seguridad de la información: organizativo, técnico y normativo. En torno a ellos se desarrollan las distintas medidas enfocadas a preservar la confidencialidad, integridad y disponibilidad de la información, en todos los ámbitos del Ministerio. El Secretario de Estado de Defensa establece con la Instrucción 41/2010 las normas para la aplicación de la Política de Seguridad de la información del Ministerio de Defensa y la Orden[57] DEF/2524/2012. Cabe destacar que el Ministerio de Defensa[58] participa en diversos grupos de trabajo nacionales e internacionales enfocados a definir una infraestructura común de seguridad de la información en el ámbito de la Administración General del Estado, la UE y la OTAN. España es, asimismo, miembro fundador del Centro de Excelencia para la Cooperación en Ciberdefensa de la OTAN, con sede en Tallin, Estonia.

La inteligencia interior: Dentro del Ministerio del Interior, podemos citar el Servicio de Información de la Guardia Civil y la Comisaria General de Información, aunque también pueden realizar labores en materia de inteligencia criminal otras unidades como la Unidad Central Operativa de la Guardia Civil y la Unidad Central de Inteligencia Criminal de la Policía. El Ministerio del Interior además, cuenta con el CNCA y el CICO, y colabora con la Unidad de Inteligencia Financiera (SEPBLAC) del Ministerio de Economía y el Servicio de Vigilancia Aduanera (SVA) del Ministerio de Hacienda y Administraciones Públicas.

Sobre este ámbito hay que señalar que los últimos sucesos de escuchas de la Agencia Nacional de Seguridad (National Security Agency, NSA) de Estados Unidos, han puesto furiosos a los países europeos, y declaran "totalmente inaceptable" este tipo de prácticas entre socios, en la declaración de la reunión de los Jefes de Estado o de Gobierno, han debatido sobre las actividades de recogida e información y la profunda inquietud que ha causado entre los ciudadanos europeos[59].

54 Vid. BOE nº 20, pp. 5700-5710. Real Decreto 199/2012, de 23 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de la Presidencia y se modifica el Real Decreto 1887/2011, de 30 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

55 España, CNI. (3 de diciembre de 2012). Norma NS/04. Seguridad de la información. Autoridad Nacional para la protección de la información clasificada. Recuperado el 4 de septiembre de 2013, del sitio web: http://www.cni.es/comun/recursos/descargas/NS-04_Seguridad_de_la_Informacion.pdf

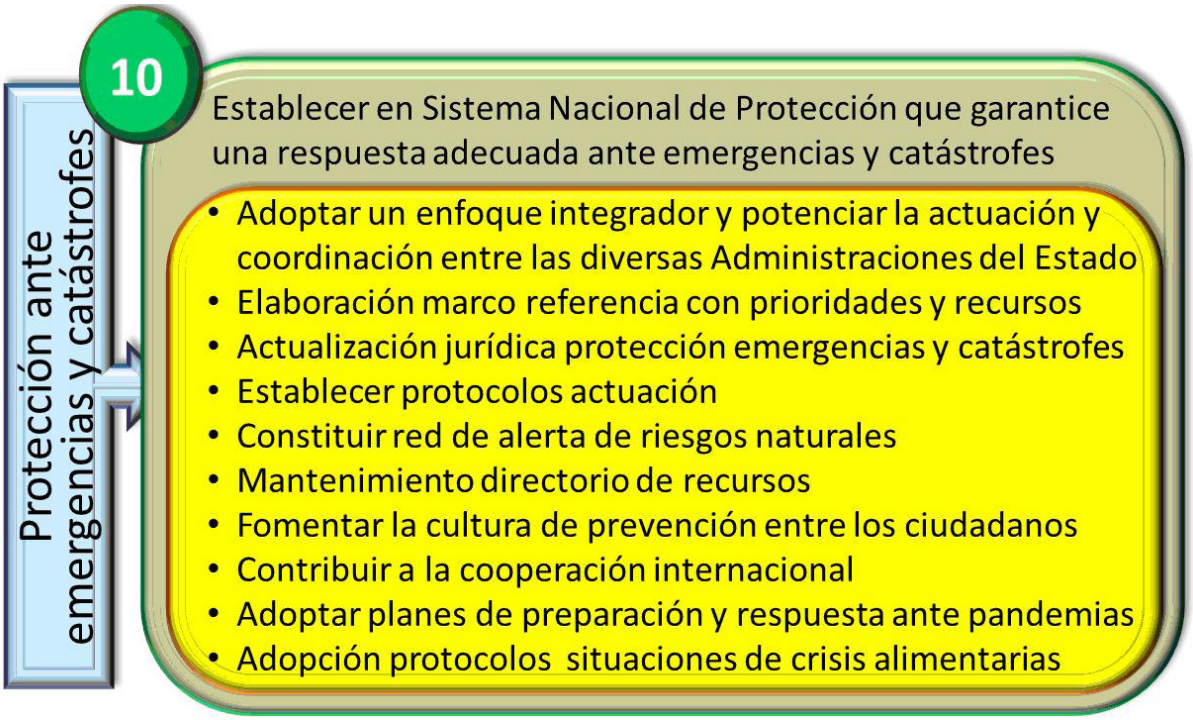
56 Vid BOD nº 103 (pp. 5856-5860). Orden Ministerial 76/2006, de 19 de mayo por la que se aprueba la política de seguridad de la información del Ministerio de Defensa.

57 Vid. BOE nº 284, Orden DEF/2524/2012, de 8 de noviembre, por la que se adecúan las normas y medidas de seguridad de la información del Ministerio de Defensa en poder de las empresas.

58 España, Ministerio de Defensa. (enero de 2013). Seguridad de la información. Recuperado el 14 de septiembre de 2013, del sitio web: http://www.defensa.gob.es/politica/infraestructura/seguridad-informacion/

59 European Union. (24 y 25 de octubre de 2013). Conclusiones del Consejo Europeo. EUCO 169/13

11. PROTECCIÓN ANTE EMERGENCIAS Y CATÁSTROFES



En este ámbito, el Ministerio del Interior tiene la Dirección General de Protección Civil y Emergencias (DGPCE), para prevenir las situaciones de grave riesgo colectivo o catástrofes, proteger a las personas y los bienes cuando dichas situaciones se producen, así como contribuir a la rehabilitación y reconstrucción de las áreas afectadas. Para responder con la mayor eficacia a las crecientes demandas de seguridad que la sociedad plantea, el Sistema Nacional de Protección Civil está en permanente evolución, por lo que se impulsa la coordinación de las actuaciones de los Órganos del Estado y la cooperación con las Comunidades Autónomas y las Corporaciones Locales. En este sentido se crea la Comisión Nacional de Protección Civil, para la citada coordinación ante situaciones de grave riesgo colectivo, catástrofe o calamidad pública[60]. Esta Comisión elabora propuestas e informes sobre programas, planes y procedimientos de actuación, que son la base para establecer la elaboración de los planes territoriales. A partir del plan territorial, se elaboran los planes especiales, para hacer frente a riesgos químicos, inundaciones, sismos, riesgo volcánico y transporte de mercancías peligrosas, y a nivel municipal, el alcalde es la máxima autoridad de protección civil sin menoscabo de las atribuciones del consejero con competencias en protección civil, ya que tiene la responsabilidad directa de los habitantes de su municipio y gestiona los recursos del pueblo o ciudad.

En el último nivel municipal, la estructura orgánica y funcional, está concebida para que se garantice la dirección única por la autoridad correspondiente, la coordinación de todas las actuaciones y se integre a los servicios y recursos propios de la administración local y regional, además de los asignados en los planes por otras administraciones públicas y entidades públicas y privadas. Cuenta con un Director del Plan, un Comité

(p. 19). Recuperado el 27 de octubre de 2013, del sitio web: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/es/ec/139219.pdf

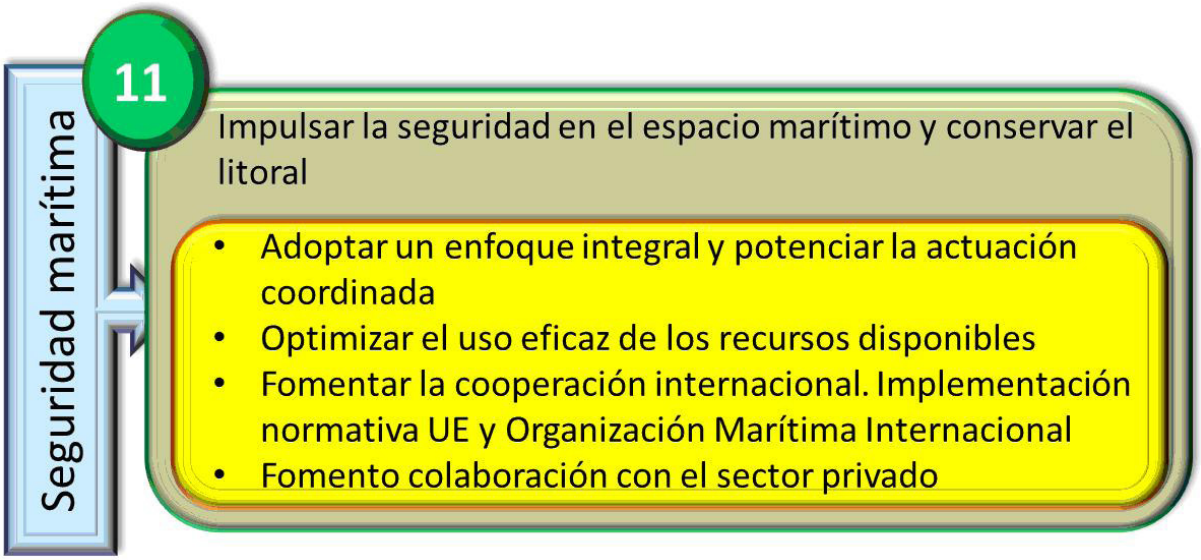
60 Vid. Ley 2/1985, de 21 de enero, sobre Protección Civil, en la que se concibe como un servicio público cuya competencia corresponde a todas las Administraciones Públicas.

asesor, un Gabinete de información y los Grupos de acción (intervención, orden, sanitario, logístico, apoyo técnico y otros.), además de los centros de coordinación (Centro de Coordinación Operativa, CECOP y Puesto de Mando Avanzado, PMA).

En las situaciones de emergencia en las que se declare el interés nacional por concurrir alguna de las circunstancias contenidas en el capítulo I (apartado 1.2) de la norma básica de protección civil, o cuando lo solicite la comunidad autónoma afectada, las funciones de dirección del Plan de Emergencia Exterior (PEE)[61], serán ejercidas dentro del correspondiente comité de dirección constituido por un representante del Ministerio del Interior y por el representante de la comunidad autónoma que determine el plan. En estas situaciones podrán acudir las Unidades de apoyo ante desastres (UAD)[62] y la Unidad Militar de Emergencias (UME)[63].

A nivel internacional corresponde a la DGPCE[64], el mantenimiento de relaciones técnicas con organismos homólogos de otros países, especialmente de la UE, del Mediterráneo y de Iberoamérica, y la participación en las reuniones de los organismos internacionales con competencias en protección civil y emergencias, así como en las comisiones y grupos de trabajo constituidos en el seno de la UE, la OTAN y Naciones Unidas. Destacando la Decisión del Consejo, de 23 de octubre de 2001 (DOUE-L-2001-82457), por la que se establece un mecanismo comunitario para facilitar una cooperación reforzada en las intervenciones de ayuda en el ámbito de la protección civil y el Dictamen de 2011, del Comité de las Regiones[65] sobre una mejor reacción europea en caso de catástrofe.

12. SEGURIDAD MARÍTIMA



61 Vid. RD 1196/2003, de 19 de septiembre, por el que se aprueba la Directriz de Protección Civil para el control y planificación ante el riesgo de accidentes graves en los que intervienen sustancias peligrosas (BOE nº 242).

62 Vid. RD 1123/2000, de 16 de junio, (BOE nº 156, de 30 de junio de 2000) mediante el cual se regula su creación e implantación. Modificado por el RD 285/2006, de 10 de marzo. (BOE núm. 70, de 23 de marzo de 2006).

63 Vid. RD 416/2006, de 11 de abril, se establece su organización y despliegue y se implanta como una fuerza conjunta de carácter permanente dentro de las Fuerzas Armadas.

64 Vid. RD 1571/2007, de 30 de noviembre, que desarrolla la estructura orgánica básica del Ministerio del Interior.

65 Vid. DOUE C 192/15-19, de 1 de julio de 2011, comunicación de la Comisión al Parlamento europeo y al Consejo sobre la reacción europea en caso de catástrofe y el papel de la protección civil y de la ayuda humanitaria

Dando cumplimiento a lo establecido en la Ley 27/1992, de 24 de noviembre, de Puertos del Estado y de la Marina Mercante, y una vez culminado el Plan 2006-2009, el Ministerio de Fomento presentó el Plan[66] Nacional de Seguridad y Salvamento Marítimo 2010-2018, desarrollado en línea con los objetivos y recomendaciones estratégicas marcados por la Política Marítima de la UE con el horizonte 2018.

Una de sus líneas de acción corresponde a la construcción de un marco de coordinación y colaboración entre actores nacionales e internacionales, Así pretenden suscribir acuerdos con el Ministerio Fiscal y las Fuerzas y Cuerpos de Seguridad, con los países vecinos, con la Agencia Europea de Seguridad Marítima (EMSA) y relación con los foros internacionales, como el Centro Regional de Respuesta de Emergencia de Contaminación Marina en el Mar Mediterráneo (Regional Marine Pollution Emergency Response Centre for the Mediterranean Sea, REMPEC), la UE, la Organización Marítima Internacional (OMI) (International Maritime Organization, IMO) , etc.

Ejemplo de la colaboración son los ejercicios[67] MARSEC, que en mayo de 2013 sirvieron para comprobar la capacidad de coordinación y colaboración de la Fuerza de Acción Marítima de la Armada con otros organismos, para afrontar operaciones de seguridad marítima, así como mejorar la coordinación en la mar entre las unidades de la Armada y las del Servicio Marítimo de la Guardia Civil, Salvamento Marítimo, Vigilancia Aduanera, Secretaría General de Pesca y Cruz Roja. Además, pretende mejorar la coordinación en la lucha contra el tráfico de drogas y la inmigración ilegal, así como conseguir una coordinación fluida entre organismos involucrados en operaciones de salvamento y rescate e incidentes que afecten a Sanidad Exterior.

El Gobierno ha querido impulsar la seguridad en el espacio marítimo, materializando el 5 de diciembre de 2013, por el Consejo de Seguridad Nacional, la aprobación de la Estrategia de Seguridad Marítima Nacional, que enumera el conjunto de intereses marítimos nacionales y recoge los riesgos y amenazas que pesan sobre ellos, ya sea por actuaciones ilegales, como el terrorismo o los tráficos ilícitos, o por las condiciones naturales del medio, como sucede con los accidentes y catástrofes[68].

Por último, destacar la implicación que tiene la Guardia Civil del Ministerio del Interior español, en la seguridad marítima, con el SIVE o el proyecto PERSEUS[69], encuadrado dentro del 7º Programa Marco de la UE, siendo evidente que la vigilancia y protección de las fronteras y los espacios marítimos es de vital importancia para garantizar la seguridad, por tratarse de un medio tan complejo y hostil como la mar, donde las fronteras se difuminan, lo que favorece el desarrollo de actividades ilícitas

66 España, Ministerio de Fomento. (2010). Plan nacional de Seguridad y Salvamento Marítimo 2010-2018. Recuperado el 7 de septiembre de 2013, del sitio web: http://www.salvamentomaritimo.es/wp-content/files_flutter/1320770125PlanNacionalSeguridad-Salvamento-Maritimo2010_2018.pdf

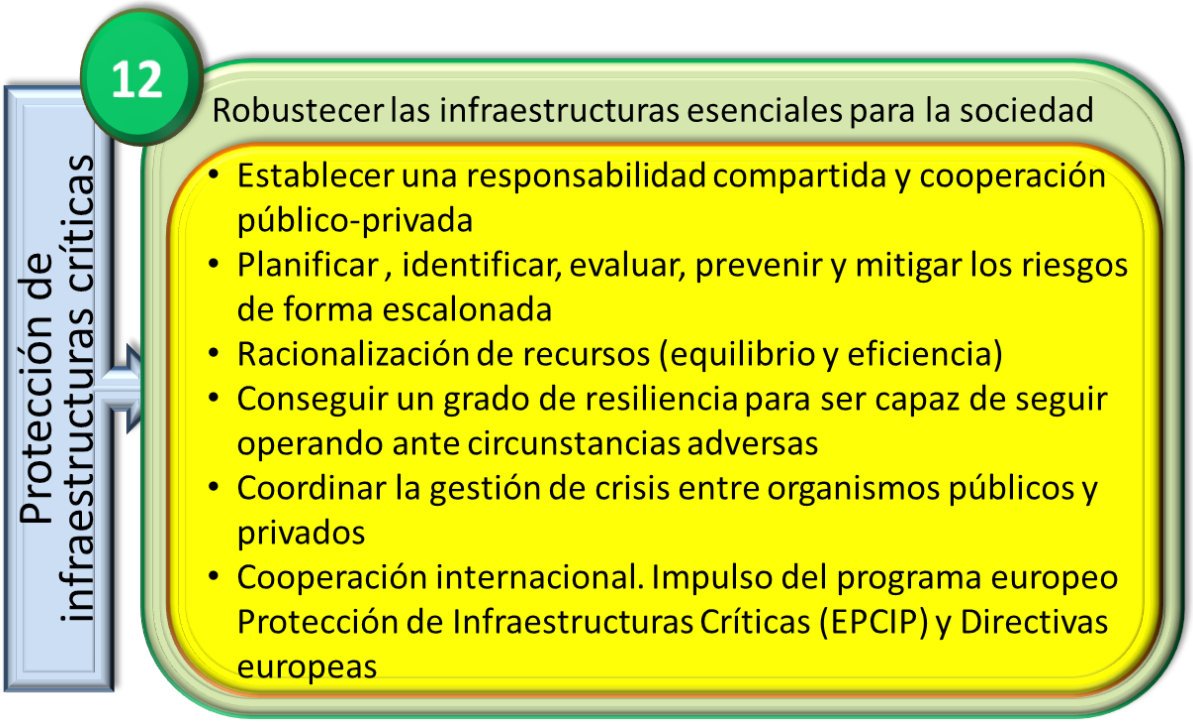
67 España, Ministerio de Defensa. (9 de mayo de 2013). Noticias de la Armada: Ejercicio Conjunto Marítimo MARSEC 13. Recuperado el 14 de septiembre de 2013, del sitio web: http://www.armada.mde.es

68 España, Consejo de Seguridad Nacional. (5 de diciembre de 2013). Nota de prensa: Aprobada la Estrategia de Seguridad Marítima Nacional de 2013. Recuperado el 6 de diciembre de 2013, del sitio web: http://www.mpr.gob.es/NR/rdonlyres/6F45B028-29F6-4862-A7B7-3B04C2AD0247/255435/20131333_completo_05dic13_1130h.pdf

69 España, Ministerio del Interior. (24 de septiembre de 2013). Intervención del ministro del Interior, Jorge Fernández Díaz, en la presentación de las primeras pruebas del proyecto PERSEUS de vigilancia marítima. Recuperado el 27 de septiembre de 2013, del sitio web: http://www.interior.gob.es/file/63/63354/63354.pdf

de cualquier tipo, y también, para ayudar a las personas en situación de riesgo.

13. PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS



En el ámbito de la protección de infraestructuras críticas, hay que señalar que es una tarea ingente intentar proteger a la sociedad contra tantas posibles amenazas, imprevisibles e inimaginables contra las infraestructuras críticas. Para ello, se requiere cooperar, compartir información, evaluar riesgos potenciales y asignar y priorizar los recursos humanos, materiales y económicos racionalmente. El reto consiste en proteger a la sociedad de los riesgos y amenazas potencialmente ilimitados, pero con recursos materiales, humanos y económicos limitados, y esto sólo es posible mediante la coordinación de esfuerzos entre todos los agentes implicados. Este es precisamente el fundamento y el impulso que pretende la Ley Protección de Infraestructuras Críticas 8/2011 y su Reglamento. Aunque el espíritu de esta ley va mucho más allá: ambiciona implantar a medio plazo una cultura de seguridad en la que tanto el sector privado como las Administraciones Públicas trabajen sobre parámetros homogéneos y claramente definidos en materia de protección de sus respectivos activos, logrando una coordinación de esfuerzos y una sinergia en sus objetivos. La citada ley establece que corresponde al Ministerio del Interior, a través de la Secretaría de Estado de Seguridad la competencia para clasificar una infraestructura como estratégica, crítica o crítica europea para incluirla en el Catálogo Nacional de Infraestructuras Estratégicas[70].

La Ley establece el Sistema Nacional de Protección de Infraestructuras Críticas que se compone de una serie de instituciones, órganos y empresas, procedentes tanto del

70 Vid. BOE nº 102 (pp. 43370-43380), de 29 de abril de 2011, Ley 8/2011 por la que se establecen medidas para la protección de las infraestructuras críticas, y BOE nº 121 (pp. 50808-50826), de 21 de mayo de 2011, Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras crítica.

sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos. Podemos destacar como agentes del Sistema a los operadores críticos del sector público y privado, es decir, aquellos que gestionan al menos una infraestructura crítica, y el CNPIC como órgano que se encarga de impulsar, coordinar y supervisar todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior en relación con la protección de las infraestructuras críticas españolas.

También la UE mantiene la preocupación sobre las infraestructuras críticas. Por ejemplo, en octubre de 2010, la Comisión Europea propuso al Parlamento Europeo una serie de medidas tendentes a reforzar la prevención, la preparación y la respuesta de la Unión ante ataques terroristas contra las infraestructuras críticas, derivadas de otra Comunicación al Consejo y Parlamento Europeo[71].

Un nuevo paso es la creación de entidades como la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)[72] en materia de seguridad de las comunicaciones. Además, en sectores como la seguridad aérea y marítima, la Comisión ha creado servicios de inspección para supervisar la aplicación de la legislación de seguridad en los Estados miembros. En diciembre de 2005, el Consejo de Justicia y Asuntos de Interior pidió a la Comisión la propuesta[73] del Programa Europeo para la Protección de las Infraestructuras Críticas (PEPIC), con el fin de definir las mismas, analizar su vulnerabilidad y su interdependencia entre sí, así como presentar soluciones que protejan y preparen para todo tipo de peligros. Dicho programa deberá ayudar a las empresas a integrar las variables de la amenaza y sus consecuencias en sus evaluaciones del riesgo. Las fuerzas del orden y de protección civil de los Estados miembros también deberían integrar el PEPIC en sus tareas de planificación e información. En este nuevo marco hay otras medidas, como el Libro Verde sobre un programa europeo para la protección de infraestructuras críticas[74], la Directiva para la identificación y designación de las infraestructuras críticas europeas (ICE)[75], o la creación de una Red de información sobre alertas en infraestructuras críticas (Critical Infrastructure Warning Information Network, CIWIN)[76].

14. CONCLUSIONES

71 European Union. (20 de octubre de 2004). Protección de las infraestructuras críticas en la lucha contra el terrorismo. COM (2004) 702 final. Recuperado el 14 de septiembre de 2013, del sitio web: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:ES:PDF

72 Vid. DOUE L 77/1-11, de 13 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información.

73 European Union. (12 de diciembre de 2006). Programa Europeo para la Protección de Infraestructuras Críticas. COM (2006) 786 final. Recuperado el 21 de septiembre de 2013, del sitio web: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:ES:PDF

74 European Union. (17 de noviembre de 2005). Libro verde sobre un programa europeo para la protección de infraestructuras críticas. COM (2005) 576 final. Recuperado el 21 de septiembre de 2013, del sitio web: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:ES:PDF

75 Vid. DOUE, L 345/75-82. Directiva 2008/114/CE del Consejo, de 23 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

76 European Union. (27 de octubre de 2008). Red de información sobre alertas en infraestructuras críticas CIWIN. COM (2008) 676 final. Recuperado el 28 de septiembre de 2013, del sitio web: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0676:FIN:ES:PDF

Del análisis realizado anteriormente, relativo al estudio de cada uno de los doce ámbitos prioritarios de actuación, relacionados con las amenazas y riesgos enumerados en la Estrategia de Seguridad Nacional (ESN-2013), y la contribución del Ministerio del Interior, podemos extraer las siguientes conclusiones:

1. El desarrollo específico de las líneas de acción enmarcadas en cada ámbito de actuación, constituye un gran reto en el que se va a enfrentar el nuevo sistema de Seguridad Nacional, impulsado por el Presidente del Gobierno con el apoyo del Consejo de Seguridad Nacional y los Comités Especializados.

2. El Sistema de seguridad integral diseñado para seguir la estrategia de la política de seguridad del Estado, necesita una organización progresiva de las estructuras y organismos del Estado vinculados a la seguridad, con la participación de múltiples ministerios, administraciones y agentes del sector público y privado.

3. El Ministerio del Interior con su estructura, está preparado para afrontar las medidas concretas que le asignen, con adecuada adaptación y mejora de sus propios sistemas de dirección y coordinación. Los contenidos totales de los ámbitos de actuación de la ESN, exceden de las competencias del Ministerio del Interior, pero es evidente que las tareas de este Ministerio y de la Secretaría de Estado de Seguridad, están relacionadas de alguna forma con los ámbitos descritos. En este sentido, las Fuerzas y Cuerpos de Seguridad del Estado (Guardia Civil y el Cuerpo Nacional de Policía) cuentan con capacidad en recursos materiales y humanos para contribuir en las líneas de acción expuestas.

4. Todos los actores implicados en la seguridad integral necesitan adaptarse a la actual situación económica, para responder con eficacia a los retos de seguridad planteados.

5. La difusión de la “cultura de seguridad” puede contribuir en la promoción de la participación ciudadana, fomentando la transparencia y aumentando la intercomunicación para evitar alguna de las amenazas descritas en la ESN.

6. La cooperación y colaboración internacional es imprescindible, primero en el marco de la UE, y después con el resto de países y organizaciones internacionales, para mejorar la capacidad de prevención y preparación frente a las amenazas emergentes, en un escenario global en constante transformación.

7. El uso de las tecnologías ha experimentado un aumento en los últimos años, derivando en la misma medida en un incremento en la cantidad y magnitud de los problemas de seguridad.

Fecha de recepción: 07/11/2013. Fecha de aceptación: 15/01/2014