PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS: SEGURIDAD ENERGÉTICA Y GUARDIA CIVIL

RAFAEL JOSÉ DE ESPONA

RESUMEN

En el nuevo marco de seguridad y defensa, la protección de las Infraestructuras Críticas requiere especial atención pues su funcionamiento es indispensable y su perturbación genera un grave impacto sobre los servicios esenciales. Las Infraestructuras Críticas energéticas son un objetivo potencial de ataques deliberados procedentes del ámbito delictivo, criminal organizado, terrorista y militar enemigo. Estas instalaciones pueden sufrir diversos impactos -aparte de los derivados de accidentes o fenómenos naturales- que afecten al sistema energético en conjunto y también a los aspectos funcionales de la Seguridad Energética. Su protección corresponde a entidades públicas y privadas y los impactos generados sobre (y a través de) ellas tienen amplios efectos sobre el sector público, la población, la economía y el medioambiente. Para dar una respuesta institucional eficaz se requieren entidades con capacidad para acometer todos los problemas de Seguridad Nacional presentes, aptas para interactuar con otras agencias involucradas. La Guardia Civil es una institución que integra las dimensiones de seguridad y defensa con competencias policiales y militares, lo cual es idóneo para la protección de las Infraestructuras Críticas y la Seguridad Energética de España.

Palabras clave: Protección de Infraestructuras Críticas, Seguridad Energética, Guardia Civil.

ABSTRACT

In the new framework of security and defense, Critical Infrastructure protection needs special attention, because its operation is is indispensable and its disfunction generates a deep impact against essential public services. Energy Critical Infrastructures are a potential target for intentional attacks coming from delinquency, criminal organisations, terrorist groups and enemy military forces. These facilities can suffer different impacts -apart of accidents and natural disasters- which concern the energy system as a whole and functional aspects of Energy Security as well. Public and private entities are responsible to protect them and the impacts generated against (and through) them have wide effects over the public sector, population, economy and environment. In order to give an efficient institucional response, it is needed to get entities able to engage all the National Security problems associated and capables to interact with other agencies involved. The Guardia Civil is a public institution which integrates security and defense dimensions having police and military functions, which is suitable to protect Critical Infrastructures and Energy Security in Spain.

Key words: Critical Infrastructure Protection, Energy Security, Guardia Civil.

1. INTRODUCCIÓN

El marco institucional y estratégico de Seguridad Nacional en España se ha reconfigurado en los 2 últimos años, ajustándose de modo acorde con el nuevo escenario internacional y funcional. La creación del Departamento de Seguridad Nacional en 2012 y del Consejo de Seguridad Nacional en 2013 fue seguida de la publicación de la Nueva Estrategia de Seguridad Nacional 2013. En el ámbito de la Comunidad de Inteligencia, ésta se ha ordenado con la reubicación del Centro Nacional de Inteligencia (CNI) en el Ministerio de Presidencia a comienzos de 2012, así como se ha procedido a la configuración del Sistema de Inteligencia Económica el cual está pendiente de ultimar. Asimismo, el establecimiento del Mando Conjunto de Ciberdefensa en el Estado Mayor de la Defensa (EMAD), también en 2013, ha actualizado la orgánica militar al más alto nivel. Quedan todavía pendientes de detallar y desarrollar algunos aspectos, además de la promulgación de legislación complementaria, que la dinámica operativa permitirá aplicar de modo eficiente.

Estas novedades institucionales no hacen sino recoger una realidad conformada por sucesivas transformaciones globales en el ámbito de la seguridad y la defensa, particularmente en los países miembros de la UE y la OTAN. La amplia proyección del concepto "seguridad" desde el año 2001, ha conllevado la inclusión de prácticamente todas las esferas de la realidad social e institucional, siendo contemplados desde la perspectiva de la seguridad. Un aspecto particularmente sensible por sus numerosas implicaciones es la energía, pues en la moderna sociedad industrial, telemática y urbana, el factor energético es la base del funcionamiento de las infraestructuras, la industria, los medios de transporte y los sistemas de comunicaciones.

En el ámbito doctrinal y programático, en la UE la Estrategia Europea de Seguridad 2003 ya destacaba hace una década la atención sobre los problemas del terrorismo, la proliferación de armas de destrucción masiva y la delincuencia organizada; este documento se complementó en 2010 con la Estrategia de Seguridad Interior de la UE integrada por 5 medidas para incrementar el nivel de seguridad europeo la cual, además de los mencionados, añadía la recomendación de aumentar la seguridad en el ciberespacio y reforzar la resistencia frente accidentes y catástrofes[1]. Por otra parte, el nuevo Concepto Estratégico de la OTAN 2010 abarca aspectos conceptuales a nivel político y estratégico, civil y militar. El nuevo Concepto Estratégico de la OTAN da comienzo a una etapa novedosa en la Alianza Atlántica, bajo una doctrina que incluye dimensiones de la seguridad y defensa de creciente relevancia no sólo para los países miembros de la OTAN sino para la comunidad internacional en general[2]. En España, la Estrategia Española de Seguridad 2011 -que supuso una novedad en cuanto a su exteriorización pública- proclamaba que "los límites entre la seguridad interior y exterior se han difuminado" por lo que la política de seguridad debe basarse en un "enfoque

1 "Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura". Comunicación de la Comisión Europea al Parlamento Europeo y al Consejo de 22 de noviembre de 2010.

2 ARTEAGA, Félix "El Nuevo Concepto Estratégico de la OTAN: lógica y estructura" ARI 2/2010, Real Instituto Elcano de Estudios Internacionales y Estratégicos. ALBERT FERRERO, Julio "Evolución del Nuevo Concepto de la Estrategia de la OTAN", Cuadernos de Pensamiento Naval nº12, Escuela de Guerra Naval, 2010; pp.7-12.

integral de las diversas dimensiones de la seguridad"[3]; desarrollando los postulados iniciales, la recientemente publicada Estrategia de Seguridad Española 2013 enumera 12 amenazas y riesgos específicos sectoriales.

En este nuevo marco doctrinal de seguridad y defensa, se perfila el concepto de Seguridad Energética con individualidad propia. Entre los documentos estratégicos descritos encontramos explícitamente la referencia a la Seguridad Energética, si bien apenas se desarrolla en su conceptuación. El citado Concepto Estratégico de la OTAN incluyó por primera vez la concreta referencia a la Seguridad Energética, la cual será configurada de un modo moderno y con visión prospectiva en el seno de la comunidad de pensamiento de la Alianza Atlántica[4], con un sentido más amplio, complejo, multivectorial y funcional que el que se había estado manejando hasta ahora y que todavía subyace a numerosos textos programáticos y normativos de los países miembros de la OTAN. Es por ello por lo que, en la pormenorización doctrinal que de la Seguridad Energética se hace en la OTAN, encontramos una conceptuación útil para el tratamiento de los aspectos de Seguridad Nacional, de manera no exclusivamente limitada a su vertiente militar.

En conjunto, podemos apreciar la tendencia de la última década a la integración funcional del binomio seguridad + defensa, con múltiples aspectos que los relacionan e incluso solapan, debido a la existencia de una serie de fenómenos acaecidos en la realidad de los últimos años:

- Gestión de crisis más compleja, con implicaciones simultáneas de orden público, protección medioambiental y estabilización económica, y métodos solutorios enfocados a la resiliencia.
- El combate asimétrico: las fuerzas armadas se enfrentan a un enemigo no convencional con armamento imprevisible (i.e. piratería) y afrontan misiones policiales en entornos de guerra. Paralelamente, las fuerzas de seguridad se enfrentan a amenazas con acciones para-militares.
- La ciberguerra: el desarrollo telemático y la integración de redes informáticas globales facilitan el espionaje y el sabotaje. (i.e. cas Wikileaks en 2010, ataques contra Estonia en 2007).
- La guerra en red: es el paradigma organizacional social, a través de la integración telemática global y la conexión de células activistas (i.e. sociales, criminales, terroristas).
- Conflictos de IV generación: con planes basados en efectos, limitación de ROEs[5] y especial atención a la estabilización post-conflicto (i.e. consolidación de gobierno y pacificación social), con gran sensibilidad al impacto informativo y a las bajas sufridas.
- La Revolución en los Asuntos Militares: con mayor tecnificación, integración

3 Estrategia Española de Seguridad 2011, Junio de 2011.

4 En el organigrama de la OTAN se ha creado la Emerging Security Challenges Division (ESCD) en 2010, el Centro de Excelencia de Seguridad Energética (NATO ENSEC CoE) en 2012 y el Smart Energy Team (SENT) en 2013 para desarrollar y pormenorizar todos los aspectos doctrinales, estratégicos y operativos de la Seguridad Energética, no sólo militar.

5 Reglas de enfrentamiento (Rules Of Encourtenment).

de sistemas, desarrollo del mando y control (i.e. sistemas C4ISR[6]), guerra electrónica y de información.

- Operaciones conjuntas y combinadas: la integración tecnológica y la vinculación de escenarios (terrestre, aéreo y marítimo) tienden al combate conjunto. La agregación de fuerzas internacionales en misiones exteriores (UE y OTAN) aumenta las operaciones combinadas.

En este contexto de seguridad y defensa, cobra especial significación el sector de las llamadas Infraestructuras Críticas. Son aquellas infraestructuras de carácter estratégico -instalaciones, redes, sistemas-equipos físicos y tecnología de la información sobre los que se basa el funcionamiento de los servicios esenciales- cuyo funcionamiento es indispensable y no permite soluciones alternativas en caso de fallo, por lo que su perturbación supone un grave impacto sobre los servicios esenciales.

Las Infraestructuras Críticas pueden sufrir diversos impactos, presentando vulnerabilidades que requieren ser cubiertas desde diversas instituciones, puesto que constituyen un objetivo potencial para ataques deliberados procedentes del ámbito delictivo común, criminal organizado, terrorista y militar enemigo (aparte de los incidentes de origen accidental o natural). Entre las Infraestructuras Críticas se cuentan, en particular, las del sector energético. La protección de las mismas y la gestión de los impactos generados sobre (y a través de) ellas exigen una alta cualificación y versatilidad de acción, habida cuenta los efectos derivados respecto de las administraciones, la población y el medioambiente.

Para una respuesta institucional eficaz ante esta problemática, se requieren entidades con capacidad para acometer todos los problemas de Seguridad Nacional asociados, aptas para interactuar con otras agencias involucradas. Entre las instituciones españolas cuyas competencias abarcan aspectos de seguridad y defensa, encontramos a la Guardia Civil como la única que integra y armoniza ambas dimensiones partiendo de su intrínseca naturaleza militar y formación castrense, con adiestramiento y operatividad policial al tiempo. Con más de un siglo y medio de tradición, la Guardia Civil tiene capacidades para una cobertura operativa en tierra, mar y aire, en tiempo de paz y guerra, en el ámbito interior y exterior y con competencias en el orden policial y militar. Es propósito del presente estudio describir los principales aspectos que acreditan como idóneo el perfil institucional y operativo de la Guardia Civil al respecto del tratamiento de aspectos de Seguridad Nacional sobre la protección de las Infraestructuras Críticas, centradas en este caso concreto en las energéticas, así como en la gestión de sus implicaciones para la Seguridad Energética de España.

2. INFRAESTRUCTURAS CRÍTICAS, SEGURIDAD Y DEFENSA

En el ordenamiento jurídico español, los artículos 8, 30 y 104 de la CE proclaman los principios de seguridad, defensa y orden público y su salvaguarda encomendada

6 Command, Control, Communications, Computers, Intelligence, Surveillance and Recognaisance. Ello permite nuevas tácticas como el Swarming combat (“guerra en enjambre”), que permiten sincronizar en tiempo real la acción, desde una aparente agregación caótica de fuerzas. ARQUILLA, John, RONFELT, David, “Swarming & the future of conflict”, RAND National Defense Research Institute, Santa Mónica (CA.), 2000.

a las Fuerzas Armadas, a las Fuerzas de Seguridad y a toda la Nación. Consecuentemente, la visión estratégica gubernamental española ha desarrollado la Estrategia Española de Seguridad 2011, la cual ha destacado que "los límites entre la seguridad interior y exterior se han difuminado" por lo que, lógicamente, la política de seguridad debe basarse en un "enfoque integral de las diversas dimensiones de la seguridad". En esta línea, la recientemente publicada Estrategia de Seguridad Española 2013 enumera 12 amenazas y riesgos específicos: conflictos armados, terrorismo, ciberamenazas, crimen organizado, inestabilidad económico-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; consecuentemente, dicho texto propone correlativas líneas de acción estratégica para afrontarlas. En la Revisión Estratégica de la Defensa se introducían, ya en el año 2003, los 14 criterios básicos para las Fuerzas Armadas (FAS), incorporando los nuevos condicionantes de la seguridad y defensa con una perspectiva de futuro, potenciando los principios de funcionalidad, proyección del poder militar y operatividad conjunta (entre los diferentes ejércitos españoles) y combinada (con fuerzas armadas de otros países). Las transformaciones del ámbito de seguridad y defensa español han coincidido con la promulgación del nuevo Concepto Estratégico de la OTAN 2010 [7].

La visión actual de la seguridad y defensa incorpora el binomio conceptual que aglutina ambas dimensiones, de modo que se trata como un término conjunto en la doctrina contemporánea. Como se puede apreciar, aparte de la retórica política y programática, se evidencia concretamente que los objetivos y misiones derivados del nuevo Concepto Estratégico de la OTAN abarcan aspectos de índole civil y militar, tanto en tiempo de paz como de guerra, especialmente en un escenario anticipado al conflicto habida cuenta la importancia de los factores disuasorios, preventivos y proactivos. La defensa deja de ser un aspecto alejado del devenir diario del ciudadano, integrándose con el plano de la seguridad interior y con aspectos tradicionalmente relegados a lo meramente policial. Ello se debe a causa de 2 fenómenos acaecidos desde la última década del siglo XX: de un lado, la llamada globalización y, de otro, la difusión de los avances tecnológicos de la informática, las comunicaciones y la telemática.

El término Seguridad Nacional conjuga hoy la seguridad y defensa en el único concepto que abarca la trascendencia de amenazas a la seguridad al plano de la defensa, incluso aquéllas que, siendo inicialmente clasificables como de seguridad interior -y gestionadas a nivel policial- se elevan a un escalón propio de la defensa. En situaciones de emergencia o catástrofe que requieren una intervención militar -sea a nivel de coordinación, apoyo o supervisión-, encontramos supuestos que crean confusión jurídica por la debida ponderación de lo que supone un riesgo de Seguridad Nacional (i.e. como se ha visto el caso de la militarización del control del espacio aéreo civil) o también cuestiones sobre conflictos competenciales y definición de la cadena de mando (i.e. como aconteció en el accidente del buque Prestige). Procede así un enfoque holístico, interdisciplinar pero jerarquizado, pues lo militar tiene capacidad de asumir la gestión del ámbito policial, pero no a la inversa. Así, la Estrategia de Seguridad Nacional 2013 realiza una definición de modo integral y amplio de la Seguridad Nacional -entendida como servicio público objeto de una Política de Estado- y fija sus

7 Aprobado en la cumbre de la Alianza Atlántica de Lisboa de 20 de Noviembre de 2010.

4 principios informadores: unidad de acción, anticipación y prevención, eficiencia y sostenibilidad en el uso de recursos y resiliencia[8].

El principio de funcionalidad ha presidido la transformación de las FAS españolas de la última década. Por contra, el clásico principio de territorialidad se ha mantenido como protagonista en el Derecho de la Guerra, pero ahora este planteamiento deviene insuficiente ante un mundo que atestigua un desarrollo tecnológico con profusión de redes de telecomunicaciones, integración telemática global e inter-dependencia económica en tiempo real. Aparecen escenarios nuevos transfronterizos o meta-territoriales en los que se proyectan problemas de seguridad y defensa, como es el ámbito cibernético. En cuanto a los medios de combate, la sociedad tecnológica y de la información genera la aparición de vulnerabilidades del Estado y la sociedad susceptibles de ser explotadas por el enemigo al margen de la utilización de armamento convencional o estratégico (i.e. disrupción del suministro energético, presión social mediante operaciones psicológicas, acciones de influencia y desestabilización política).

La Estrategia de Seguridad Nacional 2013 menciona expresamente la vulnerabilidad de las Infraestructuras Críticas como uno de los 12 riesgos concretos que recoge. Ello es acorde con la normativa europea, en particular la Directiva 2008/114/CE del Consejo, de 8 de Diciembre de 2008 sobre la identificación y designación de las infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, la cual se centra en los sectores energético y de transportes[9]. La OTAN también trata este campo con gran interés en particular[10].

Según la normativa de la UE, los Estados-miembros son los responsables en la identificación de las Infraestructuras Críticas y supervisarán las medidas de protección adoptadas. Se establece el concepto de Plan de Seguridad del Operador (PSO) donde se identificarán los elementos de las infraestructuras críticas y las soluciones de seguridad para su protección; el PSO ha de incluir, al menos, un análisis de riesgos (en base a los principales amenazas potenciales, vulnerabilidades de cada elemento y repercusión potencial), contramedidas (medidas de seguridad generales y permanentes, así como medidas de seguridad graduales activables conforme al nivel de riesgo y amenaza) y procedimientos, designándose para cada infraestructura un responsable de seguridad y enlace con las autoridades estatales. La Comisión podrá elaborar directrices metodológicas comunes para análisis de riesgos así como, junto con los Estados miembros, evaluará la necesidad de introducir medidas de protección adicionales a escala comunitaria. También se establecen directrices sobre confidencialidad de la información[11].

8 Es la Seguridad Nacional "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". Estrategia de Seguridad Nacional 2013, p.1.

9 En 2013 se ha sometido a revisión.

10 Veánse los documentos NATO EAPC, "Report on the IPC (Industrial Planning Committee) work on the protection of energy critical infrastructure" 14-12-2007 y NATO Parliamentary Assembly, 2008 Annual Session in Valencia: Committee Reports, 157 CDS 08 E rev 1 – "Energy Security: Co-operating to Enhance the Protection of Critical Energy Infrastructures".

11 PASTOR, Ignacio, "Protección de Infraestructuras Críticas: normativa nacional e internacional", ponencia del Seminario de Protección de Infraestructuras Críticas, Universidad Politécnica de Madrid, La Granja de San Ildefonso, 10-11 de Julio de 2013. VANACLOCHA BELLVER, Francisco, SÁNCHEZ GÓMEZ, José Fernando (dirs.), BREÑOSA SÁEZ DE IBARRA, Blanc, "Marco Legal y de

Siguiendo la pauta marcada desde la UE, en la normativa española la Ley 8/2011, de 28 de abril, establece las medidas para la protección de las Infraestructuras Críticas, conforme a la Directiva 2008/114/CE. El RD 704/2011, de 21 de mayo, aprueba el Reglamento para la Protección de Infraestructuras Críticas, desarrollando y concretando los contenidos de la Ley 8/2011. Conforme a su articulado, se destacan los siguientes conceptos:

- Servicio Esencial: aquél necesario para el mantenimiento de las funciones sociales básicas, la salubridad, la seguridad, el bienestar socio-económico de los ciudadanos y el eficaz funcionamiento de instituciones y administraciones públicas. Se enumeran 12 sectores con servicios esenciales: Administración, Espacio, Industria Nuclear, Industria Química, Instalaciones de Investigación, Agua, Energía, Salud, Tecnologías de la Información y Comunicaciones, Transporte, Alimentación, y Sistema Financiero-Tributario.

- Infraestructura Estratégica: es aquella instalación, red, sistema-equipo físico y tecnología de la información sobre la que se basa el funcionamiento de los servicios esenciales[12].

- Infraestructura Crítica: es aquella Infraestructura Estratégica cuyo funcionamiento es indispensable y no permite soluciones alternativas en caso de disrupción, suponiendo su perturbación un grave impacto sobre los servicios esenciales[13]. Si ello afecta al menos a 2 Estados-miembros de la UE, se denomina Infraestructura Crítica Europea. La criticidad se basa en diversos criterios (i.e. personas afectadas; impacto económico, medioambiental o público).

- Operador Crítico: es la entidad responsable del funcionamiento de la Infraestructura Crítica. Participa en el Plan Estratégico Sectorial (PES) de análisis de riesgos y elabora su propio PSO, contemplando las amenazas según análisis de riesgos, incluyendo los criterios de aplicación de medidas de protección permanente y gradual. Designa un Responsable de Seguridad y Enlace con la Administración Pública, con habilitaciones de seguridad para manejo de información clasificada. Para cada Infraestructura Crítica se elabora un Plan de Protección Específico (PPE) con medidas específicas, designando un Delegado de Seguridad. Debe garantizar la seguridad de la información clasificada y facilitar las inspecciones oficiales sobre las Infraestructuras Críticas que opera. La normativa establece contenidos mínimos para los PESs y los PSOs.

El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) subordinado a la Secretaría de Estado de Seguridad (Ministerio del Interior) es el organismo fundamental para la gestión estatal de este ámbito y tiene por función impulsar, coordinar y supervisar las actividades en este campo. Elabora el Catálogo Nacional de Infraestructuras Estratégicas y determina el carácter crítico de cada infraestructura. Dicho catálogo enumera las infraestructuras, su emplazamiento, titular y administración competente, servicio prestado, nivel de seguridad y canal de contacto. EL CNPIC opera en un entorno de información clasificada con nivel de secreto. Constituye una agencia de coordinación, con misiones de mando y control,

Gestión de las infraestructuras críticas en España", ed. McGraw-Hill, Madrid, 2013.

12 Actualmente se estima su número en unas 2.500.

13 Son aproximadamente unas 750 infraestructuras, en 2013.

protocolos de cooperación, supervisión y modernización constante, dotado de herramientas de tecnologías de la información (como el sistema de información HERMES). La Resolución de 15 de Noviembre de 2011 de la Secretaría de Estado de Seguridad establece los contenidos mínimos de los PSOs y PESs conforme a las guías de buenas prácticas publicadas por el CNPIC.

Cuestión que en un futuro próximo habrá de experimentar un desarrollo significativo son los denominados Planes de Continuidad de Servicio para Protección de Infraestructuras Críticas (BUCOPCI[14]), diseñados para fijar protocolos de operatividad alternativa en tanto el restablecimiento pleno de la situación previa al incidente en cada infraestructura.

En el campo de la protección de Infraestructuras Críticas encontramos la intervención de distintas agencias estatales y la Unidad Militar de Emergencias (UME). Junto a éstas, los efectivos de seguridad privada de que disponen los Operadores Críticos también intervienen en las actividades de protección, además de su propio personal gestor. Todo ello muestra un escenario de actividad institucional multi-agencias y de relaciones de colaboración público-privada.

Al respecto de la afectación de aspectos de seguridad y defensa, se presenta una problemática amplia al respecto de la protección de las Infraestructuras Críticas, puesto que éstas constituyen un objetivo potencial para ataques deliberados procedentes de orígenes heterogéneos, como el ámbito delictivo común (i.e. sabotaje de un empleado), el crimen organizado (i.e. extorsión), las organizaciones terroristas (i.e. atentado) y Fuerzas Armadas enemigas (i.e. ataque). Por esta razón, la atribución del incidente puede tener muy distintas repercusiones, no sólo sobre la infraestructura afectada en concreto, sino sobre la Seguridad Nacional en su conjunto.

Los medios de agresión son diversos, pudiendo abarcar desde la guerra convencional (i.e. efectuando un bombardeo de mortero), hasta el combate asimétrico (i.e. mediante dispositivos explosivos improvisados), no letal (i.e. mediante instrumentos sónicos) y cibernético (i.e. provocando una infección por virus informático)[15]. Ante la variada casuística posible, no siempre es fácil poder detectarlos ni probar irrefutablemente el haber sido empleados.

Conforme a lo explicado, se evidencia que la protección de las Infraestructuras Críticas supone un nuevo tratamiento en el contexto de las cuestiones de seguridad y defensa. Esta problemática general encuentra particularidades específicas en los distintos sectores estratégicos y sus infraestructuras asociadas, como acontece en el sector energético y en las Infraestructuras Críticas energéticas.

3. INFRAESTRUCTURAS CRÍTICAS ENERGÉTICAS Y SEGURIDAD ENERGÉTICA

En España, la Seguridad Energética ha sido recientemente resaltada como uno de los elementos del elenco de riesgos y amenazas recogidos tanto en la Estrategia de

14 Business Continuity Planning Critical Infrastructure Protection, respecto de los cuales se ha conformado un programa auspiciado por la UE, del que forman parte las entidades españolas ISDEFE y CNPIC. [http://www.bucopci.eu/index.php?option=com_content&view=article&id=1&Itemid=15].

15 Los efectos de la guerra cibernética en el ámbito de la protección de Infraestructuras Críticas han sido destacados como uno de los principales. SÁNCHEZ, Fernando José, “Critical Infrastructure Protection in Spain”, MERIDIEN, Newsletter vol.7, nº 1, Junio 2013, pp.3-5.

Seguridad Española de 2011 como en la Estrategia de Seguridad Nacional de 2013. La asunción que ésta última hace implícitamente del concepto de Seguridad Energética basado en la definición elaborada por la Agencia Internacional de la Energía -disponibilidad ininterrumpida de los recursos energéticos a un precio asumible- incide en la vulnerabilidad energética española y centra las líneas de acción sobre el abastecimiento, la distribución y el consumo[16].

España ha orientado sus organismos con competencias en materia de Seguridad Energética -como el Consejo de Seguridad Nuclear- con una visión centrada en la protección de las infraestructuras, la salud pública y el medioambiente. Ello es propio de una perspectiva clásica de la Seguridad Energética, ceñida a la custodia de las instalaciones, a la garantía de la continuidad del suministro y a la estabilidad económica. Desde esta visión, se destaca el elemento físico-territorial (plantas y conexiones energéticas) así como las relaciones comerciales de suministro y política económica. Actualmente, la doctrina moderna generada desde la OTAN[17] -el nuevo Concepto Estratégico de la OTAN 2010 menciona expresamente la Seguridad Energética por vez primera- tiende a un enfoque integrado y pluridimensional de la Seguridad Energética, el cual prima los aspectos funcionales sobre el físico-territorial. Esta nueva conceptuación contempla también los aspectos clásicos[18] y persigue la independencia y resiliencia del sistema energético, minimizando su vulnerabilidad y sensibilidad. Conjuga los ámbitos de la seguridad, defensa, economía y relaciones internacionales, con varios planos de acción sobre aspectos tangibles e inmateriales del sector energético y efectos asociados.

Por todo ello, la moderna configuración del concepto de Seguridad Energética ha de integrar todos estos elementos, de modo tal que la garantía de la continuidad del suministro sea realmente efectiva, eficiente, asumible, estable y sostenible[19]. Este enfoque funcional no menoscaba la importancia de la protección e Infraestructuras Críticas, sino que la potencia al tratarla sistematizadamente con los demás elementos del sector energético, sin aislarla.

La doctrina OTAN sobre Seguridad Energética no se ciñe al ámbito militar, siendo aplicable también al tiempo de paz y para procesos de planificación en el ámbito civil (i.e. administraciones, entidades empresariales). Las Fuerzas Armadas contribuyen a garantizar la Seguridad Energética nacional en su conjunto, al tiempo que tienen sus propias necesidades energéticas y deben proteger su propio sistema energético militar. Las Fuerzas de Seguridad asumen la primera línea de acción en materia de seguridad interior y orden público, protección medioambiental y gestión de crisis. Las amenazas tienen una génesis variada y su impacto es más lesivo -por inesperado- en situaciones

16 Estrategia de Seguridad Nacional 2013, pp. 29-30 y 45.

17 En orden a ampliar sus capacidades en este campo, en Agosto de 2010 la OTAN creó la División de Desafíos Emergentes a la Seguridad (ESCD) la cual integra, entre sus competencias, el análisis estratégico en Seguridad Energética y contempla nuevas áreas no abordadas hasta entonces, relativas tanto a la Alianza en su conjunto o a los países miembros. Es apoyada por el Centro de Excelencia de Seguridad Energética (creado en 2012 en Lituania) especializado en este campo, reforzando sus actividades con grupos de trabajo ad-hoc como el SENT (Smart Energy Team – 2013).

18 Se mantienen planes como el Plan de Emergencia Civil (CEP) de la OTAN, diseñado para la protección y seguridad de la población y directamente relacionado con la seguridad de los aprovisionamientos estratégicos, incluyendo el suministro energético.

19 DE ESPONA, Rafael José, “El moderno concepto integrado de seguridad energética”. IEEE, Documento de Opinión 32/2013, Abril 2013, disponible en: www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO32-2013_SeguridadEnergetica_RafaelJ.Espona.pdf

de normalidad. Por ello, en la protección de las Infraestructuras Críticas procede realizar una aproximación analítica desde este enfoque doctrinal, y la coordinación y sinergias entre instituciones públicas y agentes privados, el sector civil y el militar requieren que el concepto, doctrina y visión sobre la Seguridad Energética sea común.

La Seguridad Energética es un campo de gran alcance y amplitud que supera la mera securización de las Infraestructuras Críticas energéticas (aspecto que incluye) por lo que, para una adecuada protección de éstas, se requiere incardinar las medidas de prevención, predicción, reacción, recuperación y respuesta en la sistemática general de la Seguridad Energética, que es multidimensional y funcional, y se proyecta sobre todo el sector energético.

Como se ha explicado al describir el campo de la protección de Infraestructuras Críticas, el sector energético cuenta con elementos físicos básicos e instalaciones permanentes necesarios para el funcionamiento del sistema, que denominamos infraestructuras. Como se ha explicado al describir el campo de la protección de Infraestructuras Críticas, actualmente están legalmente definidos 12 sectores estratégicos de interés nacional ; en la estructura del sector energético -incluyendo todos los subsistemas energéticos (i.e. eléctrico, gasístico, petrolífero)- se engloban las infraestructuras críticas energéticas. Según la clasificación del CNPIC, éstas se agrupan en 2 de los 12 sectores estratégicos definidos: el energético y el nuclear.

En materia de Seguridad Energética, la protección de las Infraestructuras Críticas energéticas constituye una parte de las tareas que deben realizarse. Ello es así puesto que la relación existente entre la protección de las Infraestructuras Críticas y la salvaguarda de la Seguridad Energética en su conjunto debe enmarcarse dentro de la cadena de valor de la energía (desde la extracción/producción hasta el consumo).

Por otra parte, el ámbito energético presenta también una inter-relación con los demás sectores estratégicos, como ocurre especialmente en el caso del transporte (i.e. las terminales de hidrocarburos se emplazan en puertos), las telecomunicaciones (i.e. las cuales permiten la gestión de redes energéticas) y la industria química (i.e. con complejos asociados a plantas energéticas). Las Infraestructuras Críticas energéticas y la industria nuclear, respecto de la Seguridad Nacional, tienen una relación evidente no sólo para la Seguridad Energética en sí, sino también para otras dimensiones de la seguridad y el orden público (i.e. como los efectos sobre catástrofes medioambientales, el pánico en la población, la interrupción de servicios públicos o la disfuncionalidad económica).

En cuanto a la tipología de infraestructuras, existe una amplia y variada clase de Infraestructuras Críticas del sector energético, que podemos agrupar destacando principalmente 3 grupos:

- Plantas de generación, producción, extracción y transformación energética (i.e. central nuclear, refinería de petróleo, plataforma petrolífera, planta regasificadora).
- Medios logísticos de almacenamiento, transporte, distribución y terminales de acceso/salida al sistema energético (i.e. depósitos subterráneos de gas, redes de gasoductos y oleoductos, red eléctrica, terminal portuaria de GNL).
- Elementos físicos asociados (i.e. depósitos de material radiológico de deshecho).

Una implicación adicional de las Fuerzas Armadas se debe a los casos de doble utilización cívico-militar de las infraestructuras, y al marco de cooperación público-privada. Buena parte de las infraestructuras energéticas civiles sirven también al ámbito militar, aunque las FAS afrontan la salvaguarda de su propia Seguridad Energética y de abastecimiento energético autónomo. Cuando es posible y en circunstancias de paz y normalidad, también se apoyan en la infraestructura energética y en la logística civil, como un medio de aprovechamiento económico que no debe menoscabar su autonomía, diferenciación y autarquía[20] .

Se presentan también particularidades a causa de la deslocalización de infraestructuras, de los condicionantes geopolíticos y de las especificidades orográficas, con múltiples problemas técnicos, administrativos, operativos y de protección derivados del emplazamiento. Así, en la zona costera o marítima Offshore[21], se plantean cuestiones jurídico-políticas y competenciales a la hora de afrontar todos los problemas sobre la protección fronteriza, de infraestructuras, operaciones anti-piratería marítima, etc.

4. IMPACTOS Y EFECTOS SOBRE LAS INFRAESTRUCTURAS CRÍTICAS ENERGÉTICAS

Los posibles impactos susceptibles de afectar a las Infraestructuras Críticas energéticas son, en gran parte, coincidentes con los genéricos en este ámbito. Ahora bien, en la medida en que este tipo de infraestructuras tienen unas particularidades técnicas y que forman parte del sistema energético y de sus subsistemas sectoriales (i.e. eléctrico, gasístico, petrolífero), se presentan ciertas particularidades. Cabe recordar que el impacto causado sobre una Infraestructura Crítica concreta supone, además del efecto directo sobre ésta, la generación de efectos indirectos sobre el sistema al que pertenece e incluso sobre otros con los que se relaciona (i.e. en el caso de una terminal GNL portuaria, repercute sobre el sistema logístico de gas y el tráfico portuario). Partiendo de esta premisa, habrán de considerarse todas las implicaciones de los distintos tipos de impactos y efectos sobre el sector y subsectores de que se trate.

Los distintos tipos de impacto y sus consecuencias (i.e. destrucción, contaminación, bloqueo) poseen una amplia variedad de implicaciones respecto de la protección de Infraestructuras Críticas de carácter energético, que son muy sensibles (pues tratan con procesos industriales complejos y materiales inflamables y contaminantes). Partiendo de ello, se presentan numerosas implicaciones de índole institucional, funcional y de tratamiento de la información, que hacen más complejas y trascendentes las soluciones a los problemas derivados, más allá de la mera reparación y el restablecimiento operativo.

20 Como ejemplos de infraestructuras energéticas militares de gestión privada, en el caso de España se cita el oleoducto Rota-Zaragoza (ROTAZA) operado por la compañía CLH; en la OTAN está el CEPS (Central Europe Pipeline System).

21 En la costa se emplazan infraestructuras energéticas de almacenamiento y procesamiento (i.e. refinerías, depósitos), los puntos de acceso al sistema energético en muelles de atraque y terminales (i.e. petrolíferas, gasísticas de GNL) y las infraestructuras portuarias para aprovisionar energéticamente las plataformas navales civiles y militares (i.e. bunkering). En el mar se encuentran instalaciones para explotación energética (i.e. plataformas petrolíferas, terminales flotantes GNL, parques eólicos off-shore), el recorrido del tendido de los oleoductos, gasoductos y líneas eléctricas a lo largo del lecho marino (i.e. Medgaz, NordStream, NordBalt Link) y yacimientos energéticos fósiles del subsuelo marino (i.e. petróleo, gas natural).

El origen del impacto tiene su causa última bien en un hecho autónomo espontáneo o en una acción humana, lo cual condiciona el tipo de efectos generados. Así, ante un riesgo de incidente debido a un accidente fortuito (i.e. fallo técnico o humano) o un desastre natural (i.e. huracán) existe mayor imprevisibilidad de efectos. Por el contrario, frente a la amenaza de una agresión -causada por delincuente, criminal, terrorista o combatiente- se producirán consecuencias teóricamente más fáciles de predecir. Los riesgos y las amenazas han de ser considerados en sentido amplio, contemplando todo tipo de vulnerabilidades (i.e. ante ataques físicos o cibernéticos).

En cuanto a los medios, no siempre es sencillo verificar el medio empleado para la agresión, lo cual es una cuestión de gran relevancia para la resolución del problema, la definición del origen e intencionalidad del incidente y la prevención de futuras réplicas. Se plantea así la cuestión del ataque deliberado y los problemas de la verificación y la atribución[22], por lo que procede discernir si el impacto causado se debe propiamente a una agresión intencionada y clarificar cuestiones como las “operaciones de bandera falsa”, las operaciones de decepción contribuyen a complicar el escenario. Todo este proceso requiere una investigación, que se añade a las tareas de solución del incidente y de sus consecuencias.

El iter de la cadena de acciones de seguridad en el campo de protección de las Infraestructuras Críticas se divide en las siguientes fases operativas:

1. Prevención: de riesgos y amenazas, supone configurar medidas disuasorias, el establecimiento de elementos de protección, la detección de indicadores predictivos y la activación de sistemas de Alerta Temprana (i.e. en redes nacional, UE u OTAN). Rige el principio de anticipación.

2. Reacción: ante la incidencia, implica la identificación y clasificación de los incidentes (i.e. desastre natural, accidente por error humano o técnico) o agresiones (i.e. convencional, asimétrica, química, radiológica, cibernética). Cabe el señalamiento de indicadores que evidencian el origen, intención y efectos de la acción, así como la activación de los planes de emergencia y medidas reactivas (i.e. descontaminación, redireccionamiento de flujos por canales secundarios). Se orienta conforme a los principios de detección, fiabilidad y agilidad.

3. Recuperación: repara los daños y activa planes de emergencia (i.e. Planes de Continuidad de Servicio - BUCOPCIs) para la resiliencia -restablecimiento pleno del sistema- y absorción del impacto económico y medioambiental, contemplando la posible distribución de efectos en el sistema y el entorno. Se basa en criterios de adecuación y eficiencia.

4. Respuesta: contra el agresor (si existe y es identificado), cubriendo la adecuada respuesta policial o eventualmente militar, según los principios de oportunidad, proporcionalidad y congruencia.

En todo este proceso, los operadores y las agencias gubernamentales tienen distinto grado de implicación, pero se requiere un entorno cooperativo para un adecuado tratamiento del problema y todos sus aspectos (i.e. en materia de obtención y análisis de información) y también para extraer lecciones aprendidas, pues el incidente mate-

22 Recuérdese que el CNPIC orienta su funcionalidad ante amenazas relacionadas con ataques deliberados.

rializado puede aportar una serie de resultados que, en definitiva, sean beneficiosos para mejorar la protección, tales como la re-elaboración de planes de seguridad, las mejoras de procesos de coordinación entre agentes implicados, o la innovación tecnológica de contra-medidas (i.e. respecto de ataques químicos con bacterias degradantes de materiales).

En el sector energético, la orientación funcional debe prevalecer sobre la físico-territorial, sin perjuicio de articular las medidas y disposiciones conducentes a la plena protección de las infraestructuras. Recuérdese que, en materia de Seguridad Energética, el objetivo de la garantía de seguridad es, sobre todo, la continuidad de las operaciones y la resiliencia del sistema energético, más que la protección de las infraestructuras en sí mismas consideradas. Por lo tanto, en caso de producirse una agresión que provoque un costoso daño industrial, ello no necesariamente debe suponer una afectación seria del sistema (i.e. caso de una refinería); y, a contrario sensu, un impacto de meros efectos psicológicos sobre la población puede causar la paralización de todo un subsistema (i.e. el nuclear, en caso de alarma radiológica).

En el campo de la protección de Infraestructuras Críticas, se presenta una conjunción de agentes y competencias múltiples, debido a la titularidad de las infraestructuras y activos asociados (en gran parte privada o pública en régimen concesional). La operación de las infraestructuras energéticas tiende a seguir criterios de negocio por parte de las entidades empresariales, más que de servicio público. No obstante, están sometidas a la función supervisora de las administraciones públicas respecto del adecuado funcionamiento operativo de las infraestructuras, así como del impacto de las posibles incidencias en materia de orden público, salubridad, medioambiente y economía. Desde la perspectiva de la respuesta institucional a estos problemas, hay necesidad de una interacción operativa público-privada. En el proceso de planificación de la protección de Infraestructuras Críticas, los titulares de los activos (i.e. empresa energética operadora) deben trazar los PSOs y son responsables de las medidas de protección obligatorias. Pero la salvaguarda de la Seguridad Energética no se agota en esto, pues contrarrestar el elenco de amenazas no puede circunscribirse a la seguridad física. Se produce así una interacción funcional entre agencias, fuerzas de seguridad y defensa y operadores. Evidentemente, la acción institucional supera ampliamente las capacidades de seguridad industrial, pero el primer escalón y nivel de acción es de los titulares-operadores, produciéndose la mencionada interacción operativa en todo el recorrido del proceso de protección de las Infraestructuras Críticas energéticas.

Trasladando estas consideraciones a la problemática especial en el tratamiento del problema para la seguridad y defensa, se plantea la necesidad de la debida coordinación inter-agencias para garantizar la estabilidad de la población, medidas de seguridad, dispositivos de defensa, mantenimiento del orden público, protección medioambiental y continuidad operativa sectorial. Asimismo, ello es necesario para el proceso de toma de decisiones derivadas de la atribución del hecho (tareas de verificación de ataque deliberado, investigación forense y respuesta militar), la gestión de crisis y del conflicto en su caso.

La gestión de la información en tiempo real es requerida para contar con una adecuada producción de Inteligencia Crítica, con márgenes de respuesta cortos y en un entor-

no de gestión de crisis[23]. En el campo de la Seguridad Energética se afrontan problemas en un entorno de información denso y con tiempos de resolución reducidos, por lo que convine disponer de herramientas avanzadas e inter-operables para tratamiento de la información, para la protección de Infraestructuras Críticas y su interacción en el conjunto del sistema energético. La Comunidad de Inteligencia Nacional y su coordinación con agencias estatales y administraciones públicas parte de un plano metodológico común, pero no se puede soslayar la participación de las entidades privadas -compañías e industria- que están presentes en el sector energético y que operan las infraestructuras. La información útil está diseminada y su obtención es compleja, por ello conviene que los operadores dispongan de la función de Inteligencia Corporativa como adaptación de la herramienta. Esto es especialmente útil para alertas tempranas y para coadyuvar a la investigación del incidente (i.e. detección del origen del impacto), guerra de mando y control (i.e. compatibilidad entre sistemas SCADA energético y C4ISR militar), guerra de información, ciberguerra (i.e. atribución de ataques DDOS de bandera falsa), acción psicológica y comunicación pública (i.e. adecuada configuración de mensajes estabilizadores a la población para orientarla y evitar alarmismo o pánico, y contrarrestar los efectos negativos de la confusión o el pánico).

5. CAPACIDADES DE LA GUARDIA CIVIL

La protección de Infraestructuras Críticas y los efectos generados por los impactos sobre las mismas en caso de incidente suponen la afectación de la seguridad, del orden público e incluso de la defensa nacional. Durante el período inmediato al evento producido y todo el recorrido de restablecimiento de la situación, diversos órganos públicos han de intervenir para gestionar los distintos aspectos bajo su responsabilidad, con distintas capacidades y alcance competencial.

La Guardia Civil tiene varias competencias relativas al ámbito de protección de Infraestructuras Críticas. Presenta un perfil institucional idóneo para operar en este entorno con versatilidad y flexibilidad, con amplias capacidades en materia de seguridad y defensa acordes con sus caracteres diferenciales, su configuración orgánica y cometidos en materia de seguridad y defensa, salvaguarda de la integridad territorial, del orden público y de la seguridad ciudadana. Su esencial condición militar -de larga tradición y plenamente acorde con la CE de 1978- se debe a la naturaleza del instituto, al tipo de misiones encomendadas y al plus de garantía de disciplina, jerarquía, estabilidad y apoliticidad institucionales que conlleva, todo lo cual potencia su eficacia operativa.

En consonancia con la LO 2/1986, de 13 de Marzo, de Fuerzas y Cuerpos de Seguridad que explicita las funciones de la Guardia Civil, la LO 5/2005, de 17 de Noviembre, de la Defensa Nacional proclama (artículo 23) que la Guardia Civil es un instituto de naturaleza militar, con una doble dependencia del Ministerio de Defensa -con las misiones militares que le sean encomendadas- y del Ministro del Interior. Así, la Guardia Civil posee una operatividad mixta en seguridad y defensa, completada por el RD 1438/2010, de 5 de Noviembre, de desarrollo de sus misiones militares.

23 Inteligencia Crítica es aquel “tipo de inteligencia cuyo fin es satisfacer los requerimientos de inteligencia que surgen durante la gestión de una crisis”. ESTEBAN NAVARRO, Miguel Ángel (coord.), “Glosario de Inteligencia”, Ministerio de Defensa, Madrid, 2007, p.85.

La identidad institucional del Benemérito Instituto cuenta con una gran aceptación social[24], lo cual fomenta la colaboración ciudadana en materia de seguridad. El perfil orgánico y funcional de la Guardia Civil presenta unos caracteres idóneos para el campo de protección de Infraestructuras Críticas, en particular los siguientes:

- Constituye el único instituto dotado de competencias militares y policiales.
- Reviste al guardia civil de la condición simultánea de militar y agente de la autoridad.
- Tiene una idónea configuración para afrontar operaciones de combate asimétrico[25].
- Posee flexibilidad operativa, dotada de capacidad de proyección en misiones en el exterior.
- Cuenta con amplitud de recursos en inteligencia de fuentes humanas (HUMINT).
- Aquilata larga experiencia en misiones policiales y militares, de seguridad ciudadana y orden público, lucha contra el crimen organizado, protección de fronteras y antiterrorismo.
- Dispone de multi-dimensionalidad territorial -con cobertura nacional/internacional, tierra/mar/aire[26], urbana/rural- y funcional (i.e. protección de fronteras y del medioambiente).
- Percibe la amenaza con conciencia situacional y dinámicos procesos de alerta temprana.

Doctrinalmente, el pensamiento estratégico en la Guardia Civil está habituado al enfoque holístico sobre la seguridad nacional (incluyendo las dimensiones física, económica, medioambiental, etc.) en el cual ha sido pionera. Posee una perspectiva militar y civil-policial integrada, con amplia cobertura de toda la problemática de seguridad, orden público, asistencia ciudadana y protección civil.

Desde el Estado Mayor de la Guardia Civil (EMGC) se cuenta con capacidad de participar en el proceso de planificación de la defensa -incluyendo la elaboración de planes de contingencia, de gestión de crisis y operaciones militares- abarcando el escalón de planificación de seguridad civil (i.e. incidentes sobre las Infraestructuras Críticas) proyectable al nivel propio del tratamiento del conflicto militar.

Las recientes novedades normativas, orgánicas y funcionales, acaecidas entre 2010 y 2013, han supuesto que la Guardia Civil cuente de nuevo (desde el año 2012) con una Dirección General autónoma propia, potenciando sus capacidades estratégicas y operativas de modo acorde con su especificidad institucional como instituto

24 El reconocimiento social a la Guardia Civil es recurrentemente constatado por los barómetros del CIS, de modo acorde con la positiva valoración sobre las FAS en su conjunto. La Cartilla de la Guardia Civil proclama un código de honor y conducta que facilita las relaciones con la población en todos sus estratos.

25 El ahora denominado combate asimétrico fue ampliamente enfrentado desde la Guardia Civil en operaciones de contra-terrorismo y en lucha contra el bandolerismo rural y las guerrillas.

26 El Servicio Marítimo se ha dotado en los últimos años de nuevas y mejores plataformas (contando con 3 buques oceánicos) y el Servicio Aéreo ha potenciado sus unidades de ala fija (destacando los aviones CASA CN-235) y ala rotatoria, incluyendo funciones de vigilancia marítima y fronteriza.

militar con funciones policiales. El EMGC dispone de la definición normativa de las misiones militares desde 2010[27] y, con la creación del Mando de Operaciones en el año 2013, se potencia el nivel operacional. Asimismo, el desarrollo de los sistemas de información (en particular el SIGO, el SIVE y el CECORVIGMAR[28]) ha incrementado las capacidades de mando y control así como los recursos a disposición del SIGC (Servicio de Información de la Guardia Civil) el cual es parte destacada de la Comunidad de Inteligencia nacional. La reordenación de las medidas disciplinarias castrenses promulgada en 2012[29] ha sido una medida fundamental no sólo para garantizar el adecuado funcionamiento de la Guardia Civil acorde con su naturaleza militar, sino para poder interactuar más eficientemente con las FAS en su conjunto.

Tomando en consideración las transformaciones evidenciadas en el ámbito de seguridad y defensa, el contenido del nuevo Concepto Estratégico de la OTAN y la nueva Estrategia Española de Seguridad 2013, cabe destacar que la integración de la seguridad con la defensa acrecienta las limitaciones orgánicas y funcionales de los cuerpos policiales, tanto a nivel estratégico como operacional y táctico (especialmente apreciables en términos de adiestramiento, competencias, doctrina, planificación, tipología de misiones y estatuto de personal) pues los cuerpos policiales no pueden asumir funciones de carácter militar ni coordinarse eficientemente en un plano conjunto con las FAS. Por lo tanto, en un binomio integrado de seguridad y defensa, la vulnerabilidad del entorno de seguridad interior aumenta si no se cubren ambos aspectos coordinadamente. En el particular caso de España, la descentralización y asimetría regional policial (policías autonómicas) agrava la situación, además de los problemas de descoordinación inter-policial intrínsecos a toda pluralidad organizacional. Esto también es conocido en otros países de la UE y la OTAN, pues las ventajas que aporta la disponibilidad de un cuerpo militar con funcionalidad policial como la Guardia Civil no constituye un modelo exclusivo español[30].

Las características que conforman el perfil institucional de la Guardia Civil muestran un carácter propicio para estar a la altura del nuevo contexto internacional y

27 El RD 1438/2010 de 5 de Noviembre, sobre misiones de carácter militar que pueden encomendarse de la Guardia Civil, permite la integración de efectivos o unidades de Guardia Civil en estructuras militares de las Fuerzas Armadas o de una organización internacional (art. 2), a nivel estratégico, operacional y táctico ("en el planeamiento, preparación y ejecución"). Entre las actividades desarrolladas se incluyen la policía judicial, inteligencia, contrainteligencia y seguridad; enseñanza, enlace, apoyo y coordinación (art. 3). Operativamente tiende a una visión de protección y apoyo en el tipo de misiones militares descritas.

28 El sistema SIGO (Sistema Integral de Gestión Operativa) dispone de un soporte de inteligencia básica considerable, mientras que el SIVE (Sistema Integrado de Vigilancia Exterior) cuenta con medios de obtención a través de 74 estaciones sensoras (mas el Centro de Vigilancia de Frontera Terrestre de Ceuta y Melilla); el recientemente (2013) activado CECORVIGMAR (Centro de Coordinación para la Vigilancia Marítima de Costas y Fronteras) dispone de 4 centros regionales -en Valencia, Algeciras, Las Palmas y La Coruña- y centraliza la monitorización de costas y fronteras – además se integra en EUROSUR.

29 Orden General nº 9 de 22 de Noviembre de 2012, del mando, disciplina y régimen interior de las unidades. La aplicación de preceptos de las Reales Ordenanzas de Tierra y de Armada se fundamenta en la Orden PRE 1983/2012 de 14 de Septiembre, por la que se declara de aplicación a la Guardia Civil diversas normas del ordenamiento militar sobre mando, disciplina y régimen interior, aunque no siempre la jurisprudencia la ha sabido captar (STC 73/2010 y STC 122/2010).

30 Como es sabido, España no constituye el único caso de configuración orgánica de esta clase, siendo Francia -con la Gendarmerie- e Italia -con los Carabinieri- casos similares en Derecho Comparado, además de Portugal, Holanda, Rumanía, etc.

nacional de integración de seguridad y defensa, el cual se aplica a la Seguridad Energética y a la protección de Infraestructuras Críticas, puesto que tiene amplias capacidades para trabajar en el entorno de planes de seguridad, realizar investigación de hechos delictivos como atentados y sabotajes, accionar dispositivos antidisturbios, salvaguardar la protección de áreas fronterizas, intervenir en gestión de crisis y conflictos militares.

Encontramos que solamente la Guardia Civil puede cubrir todo el recorrido abarcando la investigación policial, la salvaguarda del orden público, y la respuesta policial y, en su caso, militar. Así, en materia de protección de Infraestructuras Críticas y de apoyo a la salvaguarda de la Seguridad Energética, las funciones a desarrollar por la Guardia Civil abarcan la lucha contra el terrorismo y el crimen organizado, la protección de la población y el apoyo a las FAS.

6. INTERACCIONES DE LA GUARDIA CIVIL

En el ámbito de la protección de Infraestructuras Críticas, se presenta un entorno de necesaria acción simultánea entre distintos organismos y también entre las instituciones públicas y las entidades empresariales, en tres planos de relación con frecuencia simultáneos: coordinación inter-agencias nacional [31]e internacional, cooperación público-privada entre organismos y compañías, e interacción cívico-militar tanto regular como extraordinaria[32]. Para tratar de manera sistematizada todos los aspectos y problemas que se plantean en este campo, se requiere incluir cada uno de los factores presentes de modo inteligible por parte de todos los agentes implicados, con una terminología común.

Al describir el perfil institucional de la Guardia Civil se han evidenciado las adecuadas capacidades para actuar en el entorno de protección de Infraestructuras Críticas. Esto también ocurre en cuanto al marco de agencias estatales presentes en este campo y el tipo de relaciones cooperativas que desarrollen, al respecto de las potenciales interacciones con la Guardia Civil.

La amplitud de los problemas asociados a la protección de Infraestructuras Críticas requiere un formato de trabajo inter-agencias, contemplándose al menos las siguientes con competencias aplicables al tipo de problemas que se generan en este sector: Guardia Civil, Unidad Militar de Emergencias (UME), Cuerpo Nacional de Policía, Protección Civil, Sociedad Estatal de Salvamento Marítimo (SASEMAR), policías autonómicas y policías locales, además de las FAS bajo determinadas circunstancias. A ello cabe añadir los departamentos de seguridad de los Operadores Críticos y los

31 Por ejemplo, en el ámbito marítimo-costero, actúan la Armada, el Servicio Aéreo y el Servicio Marítimo de la Guardia Civil, el SIVE, el Servicio de Vigilancia Aduanera y la Sociedad Estatal de Salvamento Marítimo.

32 Puede citarse como ejemplo de cooperación habitual civil-militar a la anteriormente mencionada compañía española CLH que gestiona el oleoducto militar ROTAZA con uso preferencial por parte de las FAS respecto de los demás usuarios civiles. Un caso paradigmático de cooperación cívico-militar extraordinaria se evidenció durante las labores de descontaminación tras la catástrofe del petrolero Prestige. RUANO GÓMEZ, Juan de Dios, “La actuación de las Fuerzas Armadas: actitudes y opiniones de la población afectada por el Prestige” Ruano Gómez, Juan de Dios (ed.), “Riesgos colectivos y situaciones de crisis: el desafío de la incertidumbre” (pp.185-218). Universidad de La Coruña, La Copruña,.2007

efectivos contratados por estos a las distintas compañías de seguridad privada y de servicios de emergencias.

Respecto del antes mencionado problema de la atribución del incidente -lo cual es cuestión clave ya que el CNPIC se orienta a hacer frente a ataques deliberados- supone la necesidad de definir, clasificar y probar los hechos para discernir su tipología (si constituye tal ataque) y poder proceder a la atribución del mismo, en paralelo a las tareas de activación y gestión de dispositivos de protección civil, acción policial y (si procede) militar. La Guardia Civil puede estar presente en toda la cadena de este proceso, a diferencia de otros organismos, pero al tiempo debe coordinarse con los demás para una eficiente acción institucional.

Así, desde que se produce el impacto sobre la Infraestructura Crítica y se ve afectado el orden público, activándose la operación de gestión de crisis -además de la investigación del incidente- la Guardia Civil interviene en el tratamiento policial con capacidad de continuar su acción a nivel militar si trascendiese a éste. Piénsese que, en caso de un ataque sobre Infraestructuras Críticas dotado de planificación militar, es muy posible que simultáneamente se realizasen en la sociedad acciones psicológicas así como actuaciones de guerra económica en otras esferas. La Guardia Civil dispone de recursos para detectar los indicadores en varios ámbitos materiales (i.e. trazabilidad de flujos financieros, infiltración de células activistas) y poder operar policial y militarmente sobre estos aspectos.

En tanto que la Guardia Civil es capaz de posicionarse en un esquema de eventos como el descrito, puede coadyuvar operativamente en todas las fases interactuando con los demás organismos competentes para cada una de las etapas o funciones públicas requeridas, tales como la dimensión marítima, aérea o terrestre; la administración local, autonómica o central, en el ámbito delictivo o bélico; con la Comunidad de Inteligencia y con las FAS

7. PROSPECTIVA Y CONCLUSIONES

Desde una visión prospectiva sobre el campo de la protección de Infraestructuras Críticas en el sector energético, consideramos que se potenciarán plausiblemente en un futuro próximo aquellos aspectos relacionados con la coordinación operativa de la respuesta al impacto infraestructural y sistémico, la investigación policial, la práctica forense y la inteligencia militar para verificar la existencia de un casus belli a partir de los incidentes sobe las Infraestructuras Críticas energéticas.

Presentan también perspectivas de desarrollo los BUPCOCIs y la mejora de capacidades en sistemas de mando y control C4ISR interoperables por distintas agencias y con apoyo de los operadores, para facilitar el trabajo en formato interorgánico y la cooperación público-privada en torno al esperado Sistema de Inteligencia Económica.

La Guardia Civil ha de contar con planes y procedimientos para coordinar sus acciones en toda la cadena de valor del sector energético, en el cual se enmarca la protección de Infraestructuras Críticas energéticas. Debemos añadir que, a nuestro juicio, considerando la competencia exclusiva de la Guardia Civil en la protección de fronteras, convendría aumentar las capacidades operativas para misiones y una mayor contribución a los procesos de planificación estratégica del Estado Mayor del

Estado Mayor de la Defensa.

A modo de recapitulación, señalamos las siguientes conclusiones:

1. El marco institucional español de Seguridad Nacional configurado desde 2012 ha incorporado nuevos órganos, inspirando su funcionalidad en el moderno concepto estratégico de los países de la UE y OTAN. Ello potencia la estructura de las FAS, las fuerzas de seguridad y la Comunidad de Inteligencia.

2. La Guardia Civil ha reforzado sus capacidades en el campo de la seguridad y defensa, reorganizando su organigrama y potenciando su operatividad en tanto que instituto militar de acción policial.

3. El nuevo Concepto Estratégico de la OTAN de 2010 introduce la Seguridad Energética en la conceptuación estratégica de la Alianza conforme a la doctrina moderna. Su visión funcional incluye la protección de Infraestructuras Críticas, con aplicación al ámbito civil y al militar.

4. La Seguridad Energética supera la mera securización de las Infraestructuras Críticas energéticas y requiere incardinar las medidas de prevención, predicción, reacción y respuesta en la sistemática general de salvaguarda de la Seguridad Energética, de modo multidimensional y funcional, sobre toda la cadena de valor de la energía.

5. Para la adecuada protección de Infraestructuras Críticas energéticas ha de tenerse en cuenta su tipología, las particularidades de su ubicación, los casos de doble utilización civil-militar y la variedad de implicaciones de cada riesgo, amenaza o incidencia sobre el sistema energético

6. La interacción entre los operadores y las agencias públicas abarca todo el proceso de protección, desde la prevención, la reacción, la recuperación y (si procede) la respuesta. En todas estas fases, la Guardia Civil tiene capacidad de acción, acorde con el hecho de que los aspectos institucionales de los agentes implicados presentan una conjunción de entes oficiales y empresariales, en un entorno nacional/internacional, público/privado y cívico/militar.

7. La Guardia Civil tiene un perfil institucional y funcional idóneo para afrontar los distintos aspectos en materia de protección de Infraestructuras Críticas en el sector energético y sus múltiples implicaciones e interacciones, con capacidad policial-militar y gran flexibilidad operativa tanto autónoma como en formato de actividad inter-agencias, en condiciones de normalidad, gestión de crisis y conflicto militar.

Fecha de recepción: 14/11/2013. Fecha de aceptación: 15/01/2014