MODELO DE CIBERSEGURIDAD EN LA ESTRATEGIA DE SEGURIDAD NACIONAL 2013

José M.ª MOLINA MATEOS
Doctor en Derecho

OS profundos cambios que está experimentando la sociedad mundial, entre los que destacan: la capacidad de los individuos de interactuar como si las fronteras no existiesen, la transmisión rápida de enormes volúmenes de información o la organización social en redes; devienen en mayores y complejos riesgos que, combinados con nuevas y variadas oportunidades, modifican el entorno estratégico internacional.

A la Seguridad Nacional, entendida como la acción del Estado dirigida a proteger la libertad y el bienestar de los ciudadanos, garantizar la defensa de España y sus principios y valores constitucionales, así como contribuir a la seguridad internacional junto con socios y aliados, no le resulta indiferente este fenómeno. Por ello, en un proceso de continuidad y revisión, se adapta y actualiza a los cambios del escenario estratégico mediante la aprobación de la Estrategia de Seguridad Nacional 2013.

La Estrategia de Seguridad Nacional (ESN) está articulada en cinco capítulos en los que, además de ofrecer un concepto de Seguridad Nacional, sitúa a la seguridad de España en el mundo, identifica los riesgos y amenazas actuales, traza los objetivos y líneas de acción estratégicas en los ámbitos prioritarios y configura un Sistema de Seguridad Nacional.

Entre los riesgos y amenazas que afectan de forma singular a la Seguridad Nacional contemplados por la ESN están incluidos aquellos que tienen una directa incidencia en el ciberespacio como nuevo ámbito de confrontación, entre los que destaca las ciberamenazas, el espionaje y las infraestructuras críticas, así como los factores potenciadores de estos, entre los que incluye la generalización del uso nocivo de las nuevas tecnologías.

La dependencia de la sociedad y del Estado del ciberespacio y su fácil accesibilidad hacen que cada vez resulten más comunes y preocupantes las

intromisiones en este ámbito. Los ciberataques, sea cual fuere su modalidad de ejecución y procedencia, se han convertido en un potente instrumento de agresión contra ciudadanos, instituciones y entidades privadas, habida cuenta que cada vez resulta más frecuente su utilización comisiva por grupos terroristas, redes del crimen organizado, empresas, individuos aislados e, incluso, por los propios Estados.

En estas circunstancias resulta esencial garantizar la integridad, disponibilidad y confidencialidad de los sistemas que soportan la prestación de los servicios mediados por las tecnologías que los sustentan y de las infraestructuras críticas que los hacen posibles.

Este entorno de información, conocimiento y tecnología resulta especialmente idóneo para ser utilizado por el espionaje con indudables éxitos que, mediante sofisticados programas, logra el acceso a ingentes volúmenes de información y datos sensibles.

Por todo ello, la Estrategia Nacional de Seguridad 2013 incluye entre sus líneas de acción específicas la *ciberseguridad* y la *contrainteligencia*. La primera, destinada a garantizar el uso seguro de las redes y los sistemas de información a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques, y la segunda, constituida por el conjunto de medidas orientadas a la defensa de los intereses estratégicos, políticos y económicos de España, para prevenir, detectar y neutralizar las agresiones encubiertas procedentes de otros Estados, de sus servicios de inteligencia, y de grupos o personas que estén empeñadas en la obtención ilegal de información.

La ciberseguridad es calificada por el propio presidente del Gobierno en el texto introductorio de la ENS «como uno de los principales ámbitos de actuación de esta Estrategia», y se articula en seis puntos:

— Incremento de la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas con el apoyo de un marco jurídico operativo y eficaz, mediante la mejora de procedimientos e impulso de recursos, con especial énfasis en:

  - Las administraciones públicas.
  - Las infraestructuras críticas.
  - Las capacidades militares y de defensa.
  - Todos los sistemas de interés nacional.

— Garantía de la seguridad de los sistemas de información, redes de comunicaciones e infraestructuras comunes a todas las administraciones públicas, para ello:

- Se completará la implantación del Esquema Nacional de Seguridad previsto en la Ley de Acceso Electrónico de los ciudadanos a los servicios públicos.
- Se reforzarán las capacidades detección.
- Se mejorará la defensa de los sistemas clasificados.
- Se fortalecerá la seguridad de los sistemas de información y de las redes de comunicaciones que soportan las infraestructuras críticas.
- Se impulsará la normativa sobre protección de infraestructuras críticas con el desarrollo de las capacidades necesarias para la protección de los servicios esenciales.

— Mejora de la seguridad y flexibilidad de las tecnologías de la información y las comunicaciones en el sector privado a través del uso de las capacidades de los poderes públicos, para lo que se impulsarán y liderarán actuaciones destinadas a reforzar la colaboración público-privada y la seguridad y robustez de las redes, productos y servicios de las TIC empleados por el sector industrial.
— Promoción de la capacitación de profesionales en ciberseguridad e impulso a la industria españolas a través de un Plan de I + D + i.
— Implantación de una cultura de ciberseguridad sólida. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.
— Intensificación de la colaboración internacional para el logro de un ciberespacio seguro y fiable en el que se salvaguardarán los intereses nacionales.

En cuanto a la estructura, el capítulo 5 de la Estrategia describe un nuevo Sistema de Seguridad Nacional en el que se establecen sus principios y objetivo principal, que ya ha sido legalizado mediante la publicación del Real Decreto 385, de 31 de mayo, de modificación del Real Decreto 1886/2011, de 30 de diciembre, por el que se establecen las Comisiones Delegadas del Gobierno.

En este Real Decreto se crea el Consejo de Seguridad Nacional, presidido por el presidente del Gobierno, cuyas reuniones serán bimestrales y tendrá competencias, entre otras, para crear comités especializados como órganos de apoyo, entre los que cabe esperar que uno de ellos sea el de ciberseguridad.

De igual modo, en su disposición final primera se incluye un mandato para que, en el plazo de seis meses desde su constitución, el Consejo de Seguridad Nacional elabore una propuesta de anteproyecto de Ley Orgánica de Seguridad Nacional, lo que es una noticia de singular trascendencia para la seguridad nacional y sería la primera de su género en la historia de España.