>> Jorge Dávila

Sobre la Estrategia Española de Seguridad

Siguiendo las pautas de otros países occidentales, nuestro país ha publicado lo que sería nuestra estrategia en temas de seguridad durante los próximos diez años. Aunque acertar con lo que se nos viene encima es trabajo de adivinadores y pitonisas, este tipo de documentos es interesante en cuanto a lo que una sociedad, o mejor dicho, sus gobernantes, creen que son sus riesgos. En este caso vamos a detenernos en conocer cuál es la galería de temores de un país desarrollado de nivel medio como el nuestro.

Con el título "*Estrategia Española de Seguridad, Una responsabilidad de todos*" [1] el Consejo de Defensa Nacional [2] aprobó el pasado 30 de mayo una iniciativa, coordinada por Javier Solana por encargo de la Moncloa, en la que se identifican los principales riesgos para la seguridad nacional para la próxima década. El objetivo del documento es encontrar los medios para garantizar la seguridad de España, sus habitantes y ciudadanos, y en él reconoce que esta tarea es propia del Gobierno, de las Administraciones Públicas y también de la sociedad en general. Lo más novedoso es reconocer a nivel oficial lo que para muchos es obvio: que "*la seguridad es hoy responsabilidad de todos*".

A la vez que reconoce que el centro de gravedad del poder en el mundo está sufriendo un claro desplazamiento desde Occidente a Oriente; también acepta como verdad insoslayable que las amenazas y riesgos son transversales, están interconectados y, desde luego, son plenamente transnacionales. Al igual que en Internet, los límites interior y exterior de las naciones se han difuminado, posiblemente, para siempre. El siglo XXI necesita enfoques defensivos completamente distintos a los seguidos en el frío y sangriento siglo anterior.

Así pues, cualquier defensa comienza con el análisis de las amenazas y los riesgos que corre nuestra seguridad. Una vez identificados la mayoría de ellos habrá que identificar líneas de respuesta y organizar los mecanismos de coordinación que permitan ponerlos eficazmente en marcha. Estos son los objetivos de la primera Estrategia Española de Seguridad (**EES**), cuyo reinado se fija en una década aunque, como es lógico, se revisará cada cinco años o cuando las circunstancias lo demanden.

Las dimensiones de análisis de la EES son: 1) afrontar el problema como un todo, 2) la coordinación de administraciones y la sociedad, 3) la eficiencia en el uso de los recursos, 4) la anticipación y prevención, 5) la resistencia y capacidad de recuperación, y 6) reconocer la interdependencia responsable con nuestros socios y aliados de la Unión Europea (UE), la OTAN y otras instituciones internacionales de las que somos socios.

Por su denominación y quizás por sus objetivos, el Sistema de Inteligencia Económica (SIE) suena a un nuevo nombre para la clásica actividad de las Agencias de Inteligencia, lo que vendría a ratificar que las guerras del siglo XXI ya solo se darán en los campos de la economía de mercado.

Ámbitos, amenazas y riesgos

Esta Estrategia pretende haber identificado las amenazas y riesgos más importantes para nuestra seguridad y señala, no siempre con claridad y concreción, cómo responder a ellas. El escenario, según la EES, está compuesto de diferentes ámbitos: el terrestre, el marítimo, el aéreo, el espacial, y el ciberespacio o el informativo. En ellos se identifican ocho grandes amenazas o riesgos, que son: 1) los conflictos armados, 2) el terrorismo, 3) el crimen organizado, 4) la inseguridad económica y financiera, 5) la vulnerabilidad energética, 6) la proliferación de armas de destrucción masiva, 7) las denominadas ciberamenazas y 8) los flujos migratorios descontrolados.

En cuanto a los conflictos armados, la EES busca conseguir su anticipación y prevención, así como su correcta y eficaz gestión, de modo que se llegue pronto a su solución y a la paz definitiva. Para ello se propone actuar multilateralmente en los frentes diplomático, militar, policial y de cooperación al desarrollo, por mencionar los más importantes. Para encargarse de todo ello se anuncia la creación de una Unidad de Respuesta Integrada Exterior (URIE).

Como es lógico, el EES reconoce como un posible riesgo el terrorismo, fenómeno heredado del siglo XX y que tan espectaculares logros tuvo al comienzo de esta década. Aunque se sigue reconociendo como riesgo, se manifiesta el hecho de que el terrorismo de ETA está en claro retroceso y que el terrorismo religioso radical islámico sigue presente pero no requiere medidas distintas a las que ya se están empleando. Después de todo, en este frente, la situación de nuestro país ha mejorado mucho respecto a lo que en su momento fue.

La EES reconoce que el crimen organizado es una de las más serias amenazas a nuestra seguridad y que es de las menos reconocidas, quizás porque los conflictos armados y el terrorismo le hacían sombra. Ahora su relación con el terrorismo, los grupos violentos y la delincuencia local consigue nuevas y peligrosas sinergias que no se deben olvidar. En este caso se propone aumentar el número de efectivos y su financiación para su combate, así como desarrollar legislaciones específicas y efectivas de alto valor disuasivo. Siguiendo lecciones ya aprendidas, también se propone mejorar la coordina-

[1] Ver http://www.lamoncloa.gob.es/NR/rdonlyres/9BD221CA-A32A-4773-ACB7-ECD3FC6C9B9E/0/ESTRATEGIAESPANOLADESEGURIDAD.pdf

[2] Según el Artículo 8 de la Ley Orgánica de la Defensa Nacional, el Consejo de Defensa Nacional es "*el órgano colegiado, coordinador, asesor y consultivo del presidente del Gobierno en materia de defensa. A iniciativa del presidente del Gobierno, podrá funcionar en pleno o como consejo ejecutivo*".

ción nacional e internacional en este ámbito y para ello se potenciaría el Centro de Inteligencia contra el Crimen Organizado (CICO), adscrito a la Secretaría de Estado de Seguridad del Ministerio del Interior.

Desde octubre de 2008, cada día nos es más evidente que la seguridad económica es condición *sine qua non* para la seguridad de los ciudadanos, las naciones y los continentes. Los últimos tres años de la economía mundial son ejemplo claro de cómo la misma actividad económica y financiera de los mercados puede ser una amenaza y un riesgo para la seguridad de los ciudadanos y las naciones. Esas amenazas tienen su origen en desequilibrios macroeconómicos, en la volatilidad y capricho de los mercados y, sobre todo, en la actuación desestabilizadora, especuladora e incluso ilegal de numerosos agentes económicos. Otros ingredientes de este peligroso cóctel son el culto pertinaz a teorías económicas falaces, la deficiente o inútil actuación de los organismos supervisores y reguladores sobre una economía global fuertemente interdependiente, la competencia por los recursos financieros escasos y un modelo de crecimiento esencialmente desequilibrado e injusto.

Terminar con esta especie de «terrorismo financiero» que los denominados "Mercados" aplican sin cuartel sobre los ciudadanos del mundo avanzado y en vías de desarrollo, requiere tanto medidas preventivas como aquellas que disminuyan los efectos de actividades especulativas que, en muchos casos, son delictivas. En la EES se reconoce que es necesario asegurar una correcta supervisión y regulación de los mercados, y que es necesario avanzar en la gobernanza económica europea y global, pero fuera de hacer esa hermosa declaración, no llega ni a insinuar el modo de hacerlo.

Dado que no parece que se vaya a cambiar de modelo económico, se habla de "*garantizar el funcionamiento de los servicios e infraestructuras críticos económicos y financieros*" pero no está claro cómo se va a hacer, sobre todo cuando las experiencias más recientes demuestran la completa incapacidad de las naciones europeas para enfrentarse a los mercados [3].

Huyendo de esa difícil tarea, el documento del gobierno español propone favorecer un "*desarrollo económico sostenible que minimice los desequilibrios y garantice el crecimiento económico y la cohesión social*", lo cual no está mal y es asumible por muchos. Sin embargo, como única medida se dice que se creará un Sistema de Inteligencia Económica (SIE) encargado de "*analizar la información relevante y facilitar la acción del Estado mediante una mejor toma de decisiones en este ámbito*". Por su denominación, y quizás por sus objetivos, el SIE suena a un nuevo nombre para la clásica actividad de las Agencias de Inteligencia, lo que vendría a ratificar que las guerras del siglo XXI ya solo se darán en los campos de la economía de mercado.

Otro elemento fundamental del conjunto de mayores riesgos que corre nuestro país es su vulnerabilidad energética. Dado que el 74% de nuestra energía primaria depende del exterior y sale de los combustibles fósiles, nuestra situación es insostenible desde el punto de vista de la seguridad. No pudiendo resolver el problema, a medio plazo se buscaría la diversificación de las fuentes de energía y el ahorro y la eficiencia energética. También se habla de "*asegurar el abastecimiento a precio razonable*" –aunque no imagino cómo lo vamos a hacer–, desarrollando reservas estratégicas y de "*la liberación de los mercados*". No sé lo qué opinará la OPEP [4] de todo esto, pero estas medidas mencionadas o bien son de difícil realización o pueden incluso ser completamente inútiles. Sin embargo, esta es una asignatura pendiente muy seria.

Internet no es precisamente el punto apto para la neutralización de ataques, sino el diseño y conexión a ella de los sistemas e infraestructuras.

Otro elemento que aparece en el documento analizado y que es uno de los objetivos del Programa de Seguridad del 7º Programa Marco de la UE es el miedo que parece haber a nivel gubernamental a la proliferación de las denominas «Armas de Destrucción Masiva». Por tales se entienden las armas nucleares, radiológicas, biológicas o químicas que, en manos incontroladas y según el EES, son "*las grandes amenazas de nuestra era*". Lo curioso es que, en principio, muchas de esas armas no existen oficialmente; a excepción del armamento nuclear, las armas químicas [5] y biológicas [6] están prohibidas. Por otra parte, en 1968, Israel ya demostró con la «Operación Plumbat» [7] cómo es posible burlar, de forma sencilla, los controles internacionales para la exportación de un material estratégico como es el uranio de calidad militar e introducirlo en su programa nuclear israelí desarrollado en Dimona [8]. Este hecho, y otros muchos ejemplos propios del contrabando, muestran lo extremadamente difícil que es controlar el tráfico de sustancias especiales, como lo son las radiactivas, y lo imposible que es ese control cuando las sustancias son de uso común, como es el caso de fertilizantes nitrogenados o pesticidas.

Aunque se han dado casos de terrorismo [9] en los que se han utilizado armas químicas, su impacto ha sido muy reducido, lo cual contrasta con el terror mediático que despierta y la importancia que le dan diferentes gobiernos. En cuanto a las armas biológicas, la situación es algo diferente, en concreto porque no depende del contrabando masivo de materias primas identificables, sino de simples "cepas"bacterianas y virales que se pueden hacer crecer y procrear en laboratorios biológicos del todo habituales. En el caso de las armas químicas su diseminación eficaz es algo bastante complicado, y en el de las armas biológicas es algo imposible de controlar. Realmente no es fácil estimar cuál es el riesgo real frente a

[3] Ver http://www.elpais.com/articulo/economia/presion/deuda/espanola/dispara/espera/cumbre/europea/elpepueco/20110711elpepueco_2/Tes

[4] **OPEP = O**rganización de **P**aíses **E**xportadores de **P**etróleo**. Ver http://en.wikipedia.org/wiki/OPEP**

[5] La **Chemical Weapons Convention** es un acuerdo de control armamentístico que prohíbe la producción, el almacenamiento y el uso de armas químicas. De hecho, su nombre completo es **Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction**.En el mes de Agosto de 2010, 188 estados habían firmado el CWC, dos la han firmado pero no ratificado (Burna e Israel) y cinco no la han firmado (Angola, Corea del Norte, Egipto, Somalia y Siria).

[6] En 1972, los EEUU firmaron la **Convención de Armas Biológicas y Tóxicas** que prohíbe el "*desarrollo, producción y almacenamiento de microbios o sus productos venenosos excepto en las cantidades necesarias para la investigación pacífica y con fines de protección*". En 1996, 137 países habían firmado ese tratado; sin embargo, se cree que desde la firma de esa Convención el número de países capaces de producir tales armas ha aumentado.

[7] Ver "**HIGH SEAS: Uranium: The Israeli Connection**", en Time Magazine, 30 de Mayo de 1977, disponible en http://www.time.com/time/magazine/article/0,9171,914952-1,00.html

[8] Ver http://en.wikipedia.org/wiki/Negev_Nuclear_Research_Center

[9] Ver http://en.wikipedia.org/wiki/Sarin_gas_attack_on_the_Tokyo_subway

este tipo de ataques, y puede estar seriamente mediatizado por lo que se quiere hacer creer y no por lo que realmente puede pasar.

No pudiendo hacer otra cosa y según la propuesta de EES, España apoyará todas las iniciativas internacionales que vayan en esa dirección, como el Tratado de No Proliferación Nuclear (TNP) y crear "*una capacidad de defensa colectiva adecuada contra la proliferación de misiles balísticos*". Este último punto es sorprendente y quizás incoherente ya que, en escenarios de terrorismo, no es probable que se utilicen misiles balísticos. Esta redacción es propia de un enfoque militar clásico de lucha entre naciones y no coincide con el escenario declarado de amenazas terroristas o de guerra asimétrica.

Ciberamenazas

Una de las novedades de la EES es la inclusión por propio derecho de las «ciberamenazas», entendidas como aquellas que, desarrolladas desde el ciberespacio, "*pueden ocasionar graves daños e incluso podrían paralizar la actividad de un país*". Hasta ahora los ciberataques solían tener fines comerciales, pero últimamente los hemos visto vinculados al *hacktivismo* [10] de nuevo cuño y no se descarta que pronto lo estén con agresiones orquestadas por grupos criminales, terroristas o, incluso, países que tienen asientos reservados en la ONU.

Para proteger la Sociedad de la Información, la EES pretende mejorar la seguridad en el ciberespacio fortaleciendo la legislación, reforzando la resistencia de las infraestructuras y agilizando la recuperación, al menos, de los sistemas de gestión y comunicación de infraestructuras y servicios críticos. El documento aboga por una absolutamente estrecha y necesaria colaboración público-privada, así como la coordinación de todos los implicados.

En la EES se reconoce que el ciberespacio y las redes de información y comunicación son fuente de nuevas posibilidades y la base de servicios muy utilizados y son parte de la gestión de infraestructuras y servicios privados, así como de servicios de las Administraciones Públicas. Por ello, hay que protegerlo y aumentar su resistencia y capacidad de recuperación. En la EES queda claro que la ciberseguridad no es sólo cuestión técnica sino "*un eje fundamental de nuestra sociedad y sistema económico*". Como ejemplo de ello, en el documento se mencionan los clásicos ciberataques a Estonia en 2007, a Georgia en 2008 y, más recientemente, a Irán en 2010, en los que una pérdida de disponibilidad puede causar daños a un país. Sin embargo, no menciona cuáles fueron las causas reales de la eficacia de dichos ataques.

En el documento se reconoce que el ciberespacio es el ámbito natural para el espionaje del siglo XXI, no solo por parte de Estado, sino también por parte de agentes criminales e incluso individuos. En el caso español, los ataques más frecuentes persiguen la obtención de información y de datos personales en la Red para ser vendidos a terceros.

La EES propone que haya una legislación común o de seguridad global que permita una lucha más efectiva contra los ciberataques, pero dudo que esa legislación vaya a tener ningún efecto dada la naturaleza de los supuestos atacantes y posibles beneficios de los escenarios de «ciber confrontación» o «ciber-sabotaje». Internet fue creada para ser útil y sencilla, y no para ser segura, por lo que la creciente interconexión de infraestructuras, suministros y servicios críticos es en sí un riesgo. Internet es y, mientras exista, seguirá siendo potencialmente anónima y, para los "iniciados", un campo en el que dificultar el rastreo de sus actividades. Precisamente Internet no es el punto apto para la neutralización de ataques, sino el diseño y conexión a ella de los sistemas e infraestructuras.

España opta por "*fortalecer la legislación, sin poner en riesgo la privacidad, y fomentar la colaboración entre el sector público y el privado*", lo cual está muy bien, y promueve sistemas de certificación voluntarios u obligatorios, así como el desarrollo de planes de contingencia. Además de ello propugna concienciar a las administraciones públicas, empresas y ciudadanos sobre los riesgos que hay, mejorar la cooperación nacional e internacional de los equipos de respuesta temprana (CERT) [11], así como elaborar bibliotecas de riesgos, catálogos de expertos, e información variada sobre recursos y buenas prácticas.

Para afianzar nuestra seguridad en el ciberespacio, la EES propone crear más medios y coordinarlos mejor, con medidas destinadas a: 1) Invertir más en tecnologías de seguridad y en la formación de personal especializado, 2) Consolidar y ampliar las líneas de acción específicas en el Plan Nacional de Protección de Infraestructuras Críticas, 3) Desarrollar el Esquema Nacional de Seguridad y realizar auditorías de la seguridad de los sistemas de la Administración, 4) Desarrollar catálogos de riesgos, expertos, recursos y de buenas prácticas, 5) Apoyar el desarrollo de empresas privadas nacionales en un sector estratégico como este dado que puede ser peligrosa la dependencia de empresas extranjeras, 6) Impulsar una educación en seguridad en el uso del ciberespacio, 7) Fomentar la formación y sensibilización acerca del desarrollo y la utilización segura de las nuevas tecnologías de la información, y 8) Promover el uso de estándares de seguridad y la certificación de los productos y sistemas tanto públicos como privados.

Nada de lo dicho anteriormente puede ser malo para la seguridad de nuestro país, de Europa y del mundo, pero no queda claro cómo se va a hacer. La formación es algo bastante descuidado en nuestros días, la inversión en tecnologías de seguridad es absolutamente marginal dentro de las actividades industriales de nuestro país, no hay acciones específicas en el Plan Nacional de Investigación que es más amplio que el de Protección de Infraestructuras Críticas, todavía no ha hecho efecto el Esquema Nacional de Seguridad ni se hacen au-

El reconocimiento a la necesidad de una ciberseguridad es ya un logro, pero todavía queda lo más difícil, que es que reconocer y entender que el origen del riesgo cibernético ésta en el erróneo planteamiento de los servicios e infraestructuras, en el incorrecto diseño de las mismas, en su pobre y precipitada implementación, en la ausencia de certificaciones serias y en que los sistemas se ponen en producción mucho antes de que se hayan mínimamente probado.

[10] Ver http://en.wikipedia.org/wiki/Hacktivismo y http://en.wikipedia.org/wiki/Anonymous_group
[11] Ver http://en.wikipedia.org/wiki/Computer_emergency_response_team

ditorías en los sistemas de la administración, no se apoya realmente el desarrollo de empresas vinculadas al territorio y a nuestra comunidad en un sector estratégico como este y asumimos desde hace años una peligrosa dependencia de empresas extranjeras [12].

La EES propugna una España "cibersegura", pues puede ser una ventaja competitiva frente a otros países y que ello atraiga a empresas de todo el mundo a localizarse aquí "*con la tranquilidad de que están operando en un entorno protegido*". Este tipo de planteamientos ponen de manifiesto que todavía no se ha asumido la omnipresencia de internet y que, en lo que a su defensa se refiere, la ubicación geográfica es irrelevante.

Cuando se trata de lo que hay que hacer en el plano internacional, la EES habla de "*impulsar la cooperación para desarrollar acuerdos de control de las ciberarmas, tal y como ocurre con las nucleares*", lo cual resulta chocante ya que nada tienen que ver las unas con las otras. El concepto de «ciber arma» que aparece en el texto es el *sumun* de la transliteración armamentística al mundo Internet y resulta ridícula. Si ya hay dificultades para controlar la exportación de toneladas de uranio con calidad militar, cómo se quiere controlar la exportación de líneas de código software que carecen de soporte material.

Después de este sobresalto terminológico, en la EES se menciona la creación de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) en 2004 pero no se dice nada sobre cuáles han sido sus resultados en "*lograr que las redes y la información de la Unión alcancen un alto grado de seguridad y* [en]*propiciar el desarrollo de una cultura de la seguridad de las redes y de la información en beneficio de toda la sociedad*".

Como último foco de riesgo, y a la vista de pateras y cayucos que llegan a nuestras costas es fácil entender el peligro que suponen los flujos migratorios incontrolados. De hecho, la misma historia de la humanidad sobre este planeta no es más que la consecuencia de numerosas migraciones masivas de seres humanos hasta llenar todo el planeta. La inmigración masiva, ilegal e incontrolada suele generar, sobre todo en tiempos de crisis, una fuerte conflictividad social que puede dar lugar a guetos urbanos y a ser el caldo de cultivo de la radicalización religiosa o ideológica. Esa miseria de los desplazados es siempre la base para la explotación económica de seres humanos por parte de organizaciones criminales. Disponer de mano de obra barata y sin derechos cívicos termina causando la desestabilización de algunos sectores productivos, el florecimiento de economías sumergidas y la falsificación de productos y mercancías.

En este caso, la EES hace propuestas más razonables y que ya se aplican, como son la colaboración entre administraciones, la cooperación con los países de origen y de tránsito, el control y vigilancia de las fronteras y la lucha contra las redes de tráfico de seres humanos.

Para terminar, la EES toma en consideración las *Emergencias y catástrofes*. Tanto si son amenazas y riesgos causados por el hombre o si su origen es natural. En este último punto resalta los efectos del cambio climático, y este tiene poco de natural. También se incluyen aquí los problemas sanitarios como las pandemias, o la escasez, en momentos determinados, de recursos básicos como el agua, la energía, el transporte, etc., ya que pueden convertirse en riesgos mayúsculos para la seguridad y el bienestar.

Se propone perfeccionar nuestra capacidad de respuesta intensificando "*la cooperación entre las Administraciones Públicas y promover una cultura de prevención entre los ciudadanos*". En este apartado se habla de la seguridad de las infraestructuras, suministros y servicios críticos que hay que garantizar y cuya capacidad de resistencia y recuperación debe ser lo más alta posible. Dado que en nuestro país todos esos servicios están en manos privadas, esta dimensión de la seguridad pasa por la leal y necesaria colaboración con el sector privado, lo cual es un objetivo a conseguir. Para todo ello se creará el Consejo Español de Seguridad que se encargará de la cooperación con las Comunidades Autónomas, e impulsará un Foro Social de Expertos como órgano consultivo.

Siempre es difícil vaticinar qué es lo que nos depara el futuro, pero las amenazas identificadas en la EES son, en mayor o menor medida, reales y, en algunos casos, probables o muy probables. Por ello, la misma existencia de la Estrategia Española de Seguridad es una buena noticia, pero todavía dista mucho de ser algo más que un discurso.

El reconocimiento a la necesidad de una ciberseguridad es ya un logro, pero todavía queda lo más difícil que es reconocer y entender que el origen del riesgo cibernético esta en el erróneo planteamiento de los servicios e infraestructuras, en el incorrecto diseño de las mismas, en su pobre y precipitada implementación, en la ausencia de certificaciones serias y en que los sistemas se ponen en producción mucho antes de que se hayan mínimamente probado. La famosa reducción a toda costa del "*time to market*" es una de las causas más importantes –pero hay otras menos confesables–, del fallo de los sistemas de información.

Solo un decidido apoyo colectivo a la industria de seguridad TIC podría hacer que nuestro país pudiese ser de algún modo atractivo para otros en estos temas de la ciberseguridad, porque en lo que se refiere a los demás frentes, nuestro tamaño como país nos coloca fuera de los primeros puestos. A pesar de todas las dificultades y todas las incomprensiones, existe una oportunidad real en el área de la ciberseguridad, que por sí misma será una pieza fundamental en la evolución del siglo XXI. ■

Solo un decidido apoyo colectivo a la industria de seguridad TIC podría hacer que nuestro país pudiese ser de algún modo atractivo para otros en estos temas de la ciberseguridad, porque en lo que se refiere a los demás frentes, nuestro tamaño como país nos coloca fuera de los primeros puestos.

Jorge Dávila Muro
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es

[12] Como le pasó a Iran con sus válvulas compradas a Siemens y para las cuales es específico el virus Stuxnet. Ver http://en.wikipedia.org/wiki/Stuxnet