CONCLUSIONES

CONCLUSIONES

POR LUIS JOYANES AGUILAR

La última quincena de noviembre de 2010 ha sido de especial interés y trascendencia para el tema central de nuestra obra dado que se han aprobado sendas iniciativas de la Unión Europea y Estados Unidos de modo conjunto y otra propia de la Unión Europea.

A la terminación de la Cumbre de la OTAN celebrada en noviembre de 2010 en Lisboa la Unión Europea y EE.UU. anunciaron la creación de un grupo de trabajo para combatir los **delitos por internet**, que consideran un problema internacional cada vez mayor. En el comunicado final de la reunión, Washington y Bruselas se declararon comprometidos con la lucha contra los delitos que se comenten por medio de **sistemas informáticos** e internet, considerados también una amenaza en el documento final de la Alianza Atlántica. El grupo de trabajo bilateral euro-estadounidense sobre «ciberseguridad» y «cibercrimen» informará de sus trabajos en el plazo de un año a las dos partes, que destacaron el éxito que han tenido en la negociación de su programa para detectar la financiación del terrorismo.

La Comisión Europea ha propuesto la creación de un Centro Europeo del Cibercrimen para el año 2013 con el objetivo de proteger mejor a ciudadanos y empresas de una nueva forma de delincuencia que, según fuentes de la CE, le cuesta a la UE cada año unos **750.000 millones de euros**. La comisaria de Interior, Cecilia Mamlström (1), ha anunciado la creación del centro contra los **delitos en la Red** que se une a la constitución del grupo de trabajo bilateral UE–Estados Unidos.

(1) Página de Cecilia Malmström, Comisaria de Asuntos de Interior: ec.europa.eu/commission_2010-2014/malmstrom/welcome/default_en.htm y europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1535&format=HTML&aged=0&language=ES&guiLanguage=en [consultado 22 noviembre 2010]

Estas dos buenas noticias en el sector de la ciberseguridad nos sirven de prólogo para la exposición final de las conclusiones de los diferentes capítulos ya citadas con anterioridad y como paso previo a las recomendaciones finales que a modo de Decálogo de intenciones proponemos como conclusión y epílogo final.

ALCANCE Y ÁMBITO DE LA SEGURIDAD NACIONAL EN EL CIBERESPACIO

La ciberseguridad afecta al bienestar digital de la sociedad, de las organizaciones y de los países y, en particular, afecta a distintas dimensiones: política, social, económica, legal, justicia y policial, técnica y de gestión. Los desafíos son complejos y afrontarlos requiere de la voluntad política para diseñar e implementar una estrategia global para el desarrollo de infraestructuras de información que incluyan una estrategia de ciberseguridad coherente y efectiva. Una respuesta firme a las dimensiones humana, legal, económica y tecnológica de las necesidades de seguridad de infraestructuras de información puede proporcionar confianza y generar un crecimiento del bienestar económico que beneficie a toda la sociedad.

La seguridad del ciberespacio es un objetivo estratégico de la seguridad nacional. El impacto de una amenaza sobre el ciberespacio tiene implicaciones sociales y económicas en el país. La próxima *Estrategia Española de Seguridad* deberá contemplar la seguridad en el ciberespacio como ya se han planteado algunos países de nuestro entorno (Gran Bretaña, entre ellos) (2)) y en particular la OTAN en la Cumbre de Lisboa celebrada el 20 de noviembre de 2010 y debería constituir el punto de partida de una *Estrategia Nacional de Ciberseguridad,* marco normativo y regulador de la seguridad en el ciberespacio. Posteriormente, debería centralizarse la gestión de la ciberseguridad con la creación de un organismo responsable de coordinar a todas las entidades públicas y privadas implicadas en España (3). Todo ello sin olvidar la cooperación internacional en esta materia y fomentar una cultura de ciberdefensa y una promoción de la I+D+i en el sector de la ciberseguridad. Los viejos problemas siguen estando presentes en esta sociedad de la información y el conocimiento y las nuevas Tecnologías de la Información y las Comunicaciones deben ayudar a resolver los citados problemas.

---

(2) Véase nota 1 del Capítulo 1.

(3) Fojón Enrique y Sanz Ángel, opus citatum.

ESTRATEGIAS LEGALES FRENTE A LAS CIBERAMENAZAS

La mutación expansiva de la categoría jurídica de seguridad nacional, que desde el concepto clásico de orden público y paz pública, seguridad interior y exterior del Estado, ha ido evolucionando hasta un concepto más amplio y multidimensional como es el de seguridad nacional. Este nuevo concepto todavía en formación, no ha acabado de perfilarse con la suficiente concreción jurídica, discurriendo en numerosas ocasiones entre su entendimiento como idea simbólica-emotiva, o como equivalente a interés general identificado con el interés del Estado y contrapuesto al interés individual. Por estas razones el usual manejo del canon de ponderación de intereses para resolver los conflictos entre seguridad nacional y derechos fundamentales, casi siempre se resuelve a favor del primero.

Existe un nuevo escenario estratégico, criminológico y político-criminal, en el que se aprecia no sólo un salto cuantitativo sino también cualitativo. Y en este sentido se habla de una ruptura: los escenarios de ataques son muy variados, con diferentes niveles de riesgo y de muy diversa escala de impacto potencial, lo que complica extraordinariamente su prevención y respuesta estatal. Ahora el *nuevo terrorismo y la nueva criminalidad transnacional*, se muestran con una mayor agresividad y representan un auténtico desafío para los Estados, pero su control, igualmente, hace peligrar los valores del Estado de Derecho, especialmente los derechos fundamentales.

El desarrollo del ciberespacio ha facilitado enormemente el desarrollo de toda clase de actividades, incluyendo interacciones comerciales, sociales y gubernamentales. El control de muchos procesos mundiales se realiza a través del ciberespacio que se ha convertido en un bien muy valioso y eso ha hecho que la seguridad del ciberespacio ha crecido en importancia.

A la profesionalización, internacionalización y globalización de la criminalidad, se suma la consolidación del uso de las tecnologías de la información y la comunicación (TIC), Las TIC constituyen instrumentos de alto valor patrimonial, político y estratégico; pero no debe minusvalorarse las facilidades su uso ofrece para la ejecución de ilícitos, lo que a su vez conlleva la generalización y aumento del recurso a estas tecnologías como instrumento comisivo.

Se puede decir que *cibercrimen* y *ciberamenazas* no son categorías equivalentes ya que existen ciberdelitos que no constituyen amenazas a la

seguridad nacional, y no todas las amenazas a la seguridad nacional nacen de la criminalidad cibernética. En los supuestos mencionados –terrorismo y criminalidad organizada–, se considera que determinadas formas de cibercriminalidad representan verdaderas amenazas a la seguridad nacional.

La combinación de varios de los factores enunciados, ha propiciado el nacimiento o el replanteamiento de una serie de complejas cuestiones jurídicas, tanto relativas a los derechos fundamentales, como a cuestiones penales sustantivas y procesales. En este sentido, la tendencia marcada por el *Convenio sobre Cibercriminalidad*, así como su funcionamiento en general, merece una valoración altamente positiva. El transcurso del tiempo y la constante innovación tecnológica han causado que el Convenio, en ciertas materias, haya quedado parcialmente obsoleto y sería necesario su actualización; este es el caso, a título de ejemplo, de conductas graves no contenidas en el Convenio, como el *phishing*, la suplantación de identidad, o los delitos cometidos en mundos virtuales. Igualmente se hace preciso reforzar y avanzar en materias como la competencia ultraterritorial en cooperación policial internacional.

EL CIBERESPACIO Y EL CRIMEN ORGANIZADO

El delincuente, y en particular el ciberdelincuente, se ha amoldado rápidamente al nuevo escenario que ha supuesto el auge de las nuevas tecnologías y el cambio en las relaciones e interacciones de la sociedad actual frente los usuarios, legisladores y gobiernos que no acaban de vislumbrar la forma de ordenar la pacífica y libre existencia.

La adaptación del ciberdelincuente a este nuevo escenario se ha manifestado en el aprovechamiento de las ventajas de las deficiencias legislativas y del nuevo espacio jurídico. Su adaptación ha sido tal que se ha procurado un espacio de impunidad, que ha supuesto un efecto llamada para la delincuencia. Han desembarcado, de la mano de los expertos informáticos o *hackers,* con toda su fuerza, abriéndose paso las formas más avanzadas de la delincuencia, las bandas organizadas.

Es necesario afrontar con decisión la delincuencia organizada que se manifiesta esencialmente en: el fraude en el comercio electrónico, en la banca electrónica, la figura del Crimen como Servicio (al estilo de los modelos de servicio en la Computación en Nube, Software como Servicio, Infraestructura como Servicio, etc.), las infraestructuras de *mulas* y los muchísimos timos en la Red.

El crimen cibernético es un negocio puro y duro, como se deduce de las declaraciones de Pilar Santamaría (4) en entrevista a *Cinco Días*: «Nosotros vemos la seguridad desde el punto de vista de los atacantes, que se organizan como empresas. No siempre los fraudes más llamativos son los más rentables. Al revés: suelen serlo los que requieren menos inversión».

LA SITUACIÓN DE LA CIBERSEGURIDAD EN EL ÁMBITO INTERNACIONAL Y EN LA OTAN

En el Ciber caso Estonia 2007, la implicación de Rusia y de ciudadanos rusos en los ataques no ofreció ninguna duda a la luz del número de evidencias recolectadas: el tráfico malicioso a menudo contenía elementos de motivación política en lengua rusa, instrucciones precisas de cuándo, cómo y qué atacar fueron diseminadas por números foros, blogs y sitios web rusos.

Pero sin duda los datos más consistente de la implicación de las autoridades rusas en el asunto, si bien no claramente como autores materiales pero sí cómo inductores, colaboradores necesarios o cómplices, son: a) la renuncia por parte del gobierno ruso a acatar el acuerdo de ayuda legal mutua con Estonia, b) la dejación de funciones por parte de las autoridades rusas en el bloqueo durante dos semanas de la embajada estonia en Moscú o en la agresión a la embajadora y c) la presión económica ejercida por Rusia coincidiendo con los ciberataques, evidenciada por el corte de la frontera a transportes pesados procedentes de Estonia, cancelaciones de contratos de importación de productos fabricados en Estonia, cancelación de transportes ferroviarios, como el que unía San Petersburgo con Tallín, etc.

– La amenaza cibernética no sólo puede afectar al normal desenvolvimiento de la vida de los ciudadanos de un país, sino que puede afectar a la infraestructura crítica nacional conllevando riesgos de daños físicos para la población.

Un ejemplo claro de esto es el «gusano Stuxnet», un código malicioso que, según los investigadores, es capaz de tomar el control de los sistemas de control automatizados de las fábricas que previamente ha infectado y puede llevar a cabo acciones para las que está programado.

(4) Pilar Santamaría, Directora de Desarrollo de Negocio y Ciberseguridad de Cisco Mediterráneo, en declaraciones a Manuel G. Pascual en *Cinco Días*, 10 de noviembre de 2010, p. 14

– El derecho a disponer de ciber armamento, es un derecho de toda sociedad democrática para poder hacer frente, con los mismos medios, a aquellos que quieren perjudicar sus legítimos intereses.

Otro ciber caso interesante, por ser el primer caso en el que se combinan operaciones militares y operaciones cibernéticas, es el Caso Georgia 2008. Como en el caso Estonia, hay hechos suficientes que inducen a pensar que el gobierno de la Federación Rusa estuvo detrás de la coordinación de las ciber operaciones, pero, a día de hoy, la demostración legal no es posible.

Por todo ello, la OTAN debe hacer un esfuerzo de renovación de acuerdo al tiempo de amenaza al que se enfrenta en la actualidad y al que se enfrentará en el futuro; y eso pasa por considerar el hecho cibernético en:

a) La definición de conceptos, estrategias, doctrinas y procedimientos.
b) En sus formas de actuación
c) En su ámbito de influencia internacional, consolidando colaboraciones y acuerdos entre la OTAN y estados No-OTAN, el sector privado y organizaciones no gubernamentales. La OTAN está en ello.

Evidentemente las consideraciones anteriores encajan plenamente dentro de la Estrategia de Ciberseguridad aprobadas en la cumbre de Lisboa de noviembre de 2010.

LA CIBERSEGURIDAD EN EL ÁMBITO MILITAR

Las TIC en el entorno militar han evolucionado desde una simple herramienta para mejorar la productividad administrativa a un medio estratégico. La amenaza a las tecnologías de la información nunca ha sido mayor y los usuarios necesitan y demandan seguridad como nunca antes había ocurrido. Los ataques pueden ser procedentes no sólo de hackers informáticos sino de terroristas, organizaciones criminales y extremistas políticos, movimientos fanáticos religiosos, servicios de inteligencia y fuerzas militares adversarias.

Los ataques cibernéticos ya no solamente tienen motivación intelectual o económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus fuerzas, además de en las dimensiones de tierra, mar y aire, a través del ciberespacio.

En el ámbito de las operaciones militares, los ciberataques también tienen que ser considerados como una amenaza, ya que cada vez resulta más probable que éstas se combinen con ataques informáticos con objeto de dejar fuera de servicio las redes y sistemas del adversario u orientar a la opinión pública a favor de uno de los contendientes.

La ciberguerra es asimétrica. El bajo coste de los equipos informáticos puede implicar que nuestros adversarios no tengan necesidad de fabricar armamento caro y sofisticado para suponer una amenaza significativa a nuestras capacidades militares.

Los sistemas en red no son los únicos susceptibles de presentar vulnerabilidades y ser atacados; tanto su software como su hardware pueden ser saboteados antes de ser unidos en un sistema en explotación. El riesgo de manipulación en el proceso de fabricación es totalmente real y es la menos comprendida de las ciberamenazas. El sabotaje es prácticamente imposible de detectar y peor todavía de erradicar.

A nivel nacional, el Ministerio de Defensa ha llevado a cabo numerosas iniciativas, publicando la Política de Seguridad de la Información, sus normas de aplicación y tomando un buen número de medidas para incrementar la seguridad de su información, tanto en el ámbito de la red de Propósito General como en el de Mando y Control.

La seguridad de la información en el Ministerio de Defensa se estructura en cinco áreas: «Seguridad de la Información en las Personas», «Seguridad de la Información en los Documentos», «Seguridad de la Información en poder de las empresas», «Seguridad de la Información en las Instalaciones» y «Seguridad de la Información en los Sistemas de Información y Telecomunicaciones», designándose Director de Seguridad de la Información del Ministerio al Secretario de Estado de Defensa, y asignándole, en el ámbito del departamento, las funciones de dirigir la seguridad de la información, velar por el cumplimiento de la política de seguridad de la información y definir y crear la estructura funcional de la seguridad de la información, incluyendo, en esta última, el Servicio de Protección de Materias Clasificadas. También se designa al Director General de Infraestructura como responsable de las áreas de seguridad de la información en las personas, en los documentos, en los sistemas de información y telecomunicaciones y en las instalaciones y como órgano de apoyo técnico para la realización de estas tareas, se designa a la Inspección General del Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de Defensa (Inspección General CIS); como

órgano de coordinación de la seguridad de la información del Ministerio, se establece, el Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa.

La formación es uno de los puntos clave para poder obtener una adecuada defensa de nuestro ciberespacio. La seguridad CIS es un campo amplísimo, que requiere de una especialización muy considerable y que además exige que dentro de ella se contemplen a la vez diversos campos de especialización.

La cifra es un aspecto imprescindible de la seguridad de nuestras comunicaciones. El uso masivo de las tecnologías de la información requiere de equipamiento de cifra acorde con las necesidades de los usuarios. Disponer de criptología nacional con seguridad verificable es un principio irrenunciable, ya que poner nuestras comunicaciones en manos de cifradores y algoritmos desconocidos o no controlados en todo su proceso de fabricación es inaceptable. Las tendencias de las nuevas generaciones de equipos de cifra son: interoperabilidad entre cifradores con diferentes redes acceso, interoperabilidad a nivel nacional y con aliados, módulos reprogramables y certificación múltiple.

El mercado de productos de cifra es reducido, limitado casi exclusivamente a la Administración General del Estado y existen pocas empresas nacionales que desarrollen productos cripto, que además son de tamaño y facturación pequeños, por lo que seria necesario un esfuerzo de desarrollo y que éste sea sostenible en el tiempo.

Consideramos que la Unión Europea debería desarrollar una estrategia similar a la contenida en la Iniciativa Nacional de Ciberseguridad de Estados Unidos. En ella se fija el objetivo de establecer estrategias efectivas para blindar las transacciones bancarias y financieras, las redes de transporte por superficie, subterráneas, aéreas y marítimas, y la protección digital de las infraestructuras de comunicaciones civiles y militares, de energía, transporte, seguridad militar, e informática, de toda la nación. Se pretende con evitar que los ciberatacantes provoquen apagones masivos, detengan la actividad comercial y financiera, cometan fraudes a particulares y entidades financieras, o alteren el funcionamiento de las redes de seguridad informáticas civiles y militares.

Esta misma orientación ha tomado la doctrina militar rusa en materia de seguridad en la información, como se ha publicado parcialmente en febrero de 2010 en un documento no clasificado.

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD. CIBERTERRORISMO

Los ciberataques son muy rentables en términos de esfuerzo necesario para su ejecución, riesgos que se asumen y beneficios económicos o políticos que se pueden obtener y afecta transversalmente tanto al sector público, al sector privado como a los ciudadanos. Además no existe una legislación armonizada que permita una lucha efectiva contra estas amenazas

Como ya hemos considerado anteriormente, todas las naciones de nuestro entorno están desarrollando iniciativas para intentar controlar las amenazas que vienen del ciberespacio y la mayoría de ellas está apostando por estructuras similares a la propuesta en el capítulo 6.

En España las responsabilidades en el ciberespacio están muy fragmentadas en diferentes organismos que abordan el problema de forma parcial.

Es necesario por tanto impulsar actuaciones en este sentido fortaleciendo las capacidades de respuesta ante incidentes y de inteligencia ante este tipo de amenazas. La dotación presupuestaria se considera crítica si se quieren llevar a cabo las líneas de acción que se plantean como posibles soluciones para reducir la amenaza.

Por ello, la estrategia propone que se establezca un programa que afecte a todo la nación para alcanzar los objetivos estratégicos planteados incrementando los fondos que desarrollen nuevas tecnologías para proteger las redes nacionales e incrementando la formación en perfiles críticos para esta actividad y fomentando el trabajo coordinado entre el sector público, la industria, los ciudadanos y los aliados internacionales.

PROPUESTAS A MODO DE DECÁLOGO DE LA CIBERSEGURIDAD

Teniendo presentes los análisis y conclusiones realizadas en la ntroducción y los diferentes capítulos de nuestra obra y la aprobación de la Estrategia de Ciberseguridad realizada por la OTAN en la Cumbre de Lisboa del 20 de noviembre de 2010, haremos una propuesta de reflexiones que consideramos fundamentales para el futuro desarrollo de una estrategia de Ciberseguridad Nacional teniendo presentes los retos, oportunidades y amenazas en el contexto de la seguridad nacional;

1. Sería conveniente alcanzar un Sistema Normativo Europeo y Nacional que se adapte con rapidez a la situación cambiante de los riesgos TIC de modo que incluya sanciones para los nuevos delitos provenientes de los ataques informáticos. Las iniciativas de algunos países de nuestro entorno europeo ya examinadas en la obra y la ya citada aprobación de las estrategias de ciberseguridad de la OTAN, pueden ser elementos de apoyo y ayuda a la elaboración del propuesto sistema normativo europeo y nacional.
2. Establecer una plataforma española de ciberseguridad y la posibilidad de crear un Centro Español de la Ciberseguridad dependiente de una Dirección única que actúe de modo centralizado y alineada con las estrategias europeas emanadas de la Agenda Digital Europea (5).
3. Aunar esfuerzos en ciberseguridad a nivel nacional e internacional mediante el intercambio de experiencias y conocimientos. Las experiencias realizadas en Cyber Europe 2010 y las realizadas en España (Ejercicios de Ciberdefensa de las FAS) pueden ser también elementos de referencia,
4. Fomentar la cultura de ciberseguridad en todos los niveles: administración, industria, empresas y ciudadanos (adultos y sobre todo menores).
5. Fomentar la colaboración público-privada en el campo de la seguridad y las infraestructuras críticas, fomentar la modernización tecnológica y en trabajar en aumentar la confianza en los servicios de Seguridad de la Información y las TIC (Tecnologías de la Información y la Comunicación).
6. Fomentar la I+D+i en Seguridad de las TIC (STIC).
7. Alinear los enfoques académicos de seguridad con los nuevos escenarios de amenazas y riesgos TIC.
8. Abogar por una estrategia de ciberseguridad que se traduzca en Sistemas de Gestión de Seguridad de TIC que consideren la Gestión de Riesgos TIC aplicando metodologías pertinentes.
9. Caminar hacia la Gobernanza de las TIC que supone poder gestionarlas adecuadamente, mediante el desarrollo de mecanismos y toma de decisiones que estén alineadas con las prioridades y líneas de las estrategias y control de riesgos TIC.

(5) Acciones clase 7 y otras acciones, en *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones.* ***Una Agenda Digital para Europa*****.** Bruselas, 26.8.2010 COM(2010) 245 final/2. pp. 20-21.

10. La formación es uno de los puntos clave para poder obtener una adecuada defensa de nuestro ciberespacio y alcanzar una mentalidad de la Ciberseguridad como activo nacional. Para ello las diferentes administraciones debería promover en los planes de estudio de los diferentes escalones educativos la introducción de materias relativas a la ciberseguridad.

Para terminar debemos considerar la necesidad de alineamiento de la estrategia nacional de ciberseguridad con la regulación que en materia de TIC ha aprobado la Unión Europea en su *Agenda Digital para Europa* puesta en marcha en la Declaración de Granada realizada en la reunión de ministros europeos de Telecomunicaciones celebrada en febrero de 2010 en la ciudad de Granada y aprobada y publicada posteriormente.

En particular la Comisión declara en su *acción clave 7* que:

> *«Presentará medidas, incluyendo iniciativas legislativas, para combatir los ciberataques contra los sistemas de información a más tardar en 2010, y una normativa conexa sobre la jurisdicción en el ciberespacio a nivel europeo e internacionala más tardar en 2013» y en otras acciones: «Establecerá una plataforma europea de la ciberdelincuencia a más tardar en 2012» y «Examinará, a más tardar en 2011, la posibilidad de crear un centro europeo de la ciberdelincuencia».*

Entendemos que, el Gobierno de la Nación, como por otra parte ya lo está haciendo, deberá seguir liderando las estrategias en ciberseguridad e iniciar una concienciación y una campaña de educación para promover dicha ciberseguridad.