Conclusiones de una conciencia de *ciberseguridad* y *ciberdefensa*

La esperanza tiene dos preciosos hijos: sus nombres son enfado y valor; enfado al ver cómo son las cosas y valor para no permitir que continúen así

San Agustín

La elaboración de las conclusiones de esta monografía es desarrollada a título estrictamente personal después de una reflexión detallada de los cinco documentos que la componen.

Vivimos momentos especialmente interesantes para una reflexión como la que se ha llevado a cabo en este trabajo. La noticas sobre *ciberseguridad* inundan los espacios informativos y se considera, en las estrategias de seguridad de todos los países, incluido el nuestro, que la *ciberseguridad* es un elemento clave a tener en cuenta para el desarrollo de una sociedad civil adecuadamente formada, de unas empresas con formación y tecnologías suficientes de prevención ante los incidentes derivados de la misma y de una Administración Pública dotada de tecnologías y formación para prestar al ciudadano los servicios públicos que se necesitan con garantías suficientes y que permita que la ciudadanía se relacione con la Administración de forma segura y confiable, avanzando, como en el caso de España, en el desarrollo de la agenda digital. Parte fundamental de esta agenda digital es la *ciberseguridad*.

Es el momento adecuado para progresar en el desarrollo de una estrategia de *ciberseguridad* donde, además de detallar los riesgos, las amenazas y las vulnerabilidades, se trate a aquella como un elemento tractor de la industria especializada de la información. También es forzoso abordar los papeles que tienen que desarrollar los distintos actores de la Administración, incluido el tema fundamental, el de la gobernanza. Para que esta estrategia se consolide, necesita abordar como elemento vertebrador la relación público-privada, siendo esta última el elemento que permite actuar sobre las amenazas y los riesgos de una forma rápida y en continuo movimiento. Si algo caracteriza a este sector es el cambio continuo y, para prevenir y actuar contra los ataques, es necesaria una flexibilidad que aporta el sector privado. La necesidad de abordar una política de I+D nacional en este área es fundamental para desarrollar tecnologías que permitan una vida ordenada en este espacio de posibilidades que es el ciberespacio.

Intentar describir la inquietud ante la necesidad de vertebrar elementos público-privados en el desarrollo de las capacidades de *ciberseguridad*, inteligencia y seguridad económica de nuestro país para el fortalecimiento de nuestra posición en el mercado internacional, el desarrollo de la competitividad del tejido industrial, la seguridad de la economía y de las empresas y el refuerzo de la influencia de nuestro país no es algo nuevo.

En el caso de los intervinientes en este trabajo, los evangelizadores, ha sido una labor de comunicación continuada durante muchos años intentando hacer comprender el escenario que se nos avecinaba, avanzando en todas nuestras intervenciones, la necesidad de concienciar a la Administración, a las empresas y a los particulares sobre las amenazas, los riesgos y las oportunidades que este nuevo modelo de interrelación social iba a generar.

Acaba de ser publicada la Estrategia Nacional de Seguridad para España y estamos a la espera de que vea la luz la Estrategia Nacional de Ciberseguridad. Un mundo que no deja de avanzar de una forma cada vez más acelerada donde el análisis de los acontecimientos nos hace modificar nuestras percepciones y los modelos con los que tradicionalmente habíamos entendido la realidad. Es por ello que dichas estrategias son elementos vertebradores fundamentales para el posicionamiento de nuestro país en la esfera internacional y permiten desarrollar las bases y los objetivos y esbozar el recorrido para alcanzar ese fin.

La crisis económica, los conflictos sociales, los nuevos escenarios de guerra económica, las situaciones de nuevos espacios de confrontación son parte sustancial de nuestra vida diaria. Pero, del mismo modo, aparecen nuevas oportunidades que permiten comprender por qué las grandes crisis proporcionan nuevas vías de expresión del ser humano, elabo-

rando nuevas construcciones de entendimiento de nuestro presente y de nuestro futuro.

Hablar de *ciberseguridad*, en estos últimos trece años, ha sido la prédica de la anticipación de una revolución tecnológica que iba aparejada a un nuevo modelo de cambio social. La tecnología de Internet ha proporcionado un nuevo paradigma de la comunicación social, rompiendo las dimensiones clásicas del espacio y el tiempo. La tecnología que posibilita este cambio también permite que se desarrollen capacidades que generan amenazas para las que ni países ni empresas ni individuos estábamos preparados. Por ello, esa labor de comprensión del nuevo entorno necesita nuevas herramientas de estudio, de formación y de colaboración entre todos los agentes sociales tanto públicos como privados.

La colaboración público-privada es reconocida por todos como la única vía de abordar esta situación. La gestión de los riesgos, las amenazas, la prevención de estos elementos y el desarrollo de la capacidad de reacción ante una alerta temprana frente a incidentes se demuestra como estratégica en el mantenimiento de la integridad tanto de individuos como de empresas y estados. Nadie está excluido del riesgo, por este motivo la necesidad de concienciación de estos riesgos es de obligado cumplimiento.

Las manifestaciones en la red del crimen organizado, del proselitismo terrorista, de la acción terrorista, del ataque contra los activos intangibles de las empresas mediante el espionaje a través de *advanced persistent threats,* y del riesgo de los ciudadanos, especialmente los jóvenes frente al acoso bajo sus distintas manifestaciones, ha hecho que palabras como *ciberseguridad, ciberterrorismo, ciberataques, ciberdefensa, ciberacoso*... se instalen en nuestra semántica diaria.

Los procesos de convergencia de las distintas seguridades ya es algo cotidiano. La realidad presenta situaciones para resolver esas aparentes contradicciones. La Ley de Protección de Infraestructuras Críticas genera un espacio de diálogo entre los responsables de seguridad de las organizaciones para consolidar un único interlocutor frente a riesgos que provienen de dos espacios distintos, «el físico y el lógico», pero esa categorización tiene menos sentido cuando lo que realmente importa es la prevención de los riesgos y la gestión de las amenazas, cuando se pone el objetivo en lo que nos une más que en lo que nos separa. No hay espacios limitativos ya que la **seguridad** sí es una tarea de todos.

Los años de análisis sobre este tipo de cambio social que empezamos algunos en el año 1982 y que en los últimos años hemos venido anticipando nos han permitido «evangelizar» sobre los riesgos inminentes que se cernían sobre nuestro día a día si no nos concienciábamos de la necesidad de entender y prevenir los riesgos y convertirlos en oportunidades para, entre otras cosas, generar en España un tejido industrial de

primer orden que pudiera poner a disposición de las empresas, de las personas y de la Administración unas tecnologías «marca España» que posibilitaran la percepción de la Seguridad como elemento constitutivo de nuestro día a día.

Vivimos en un mundo complejo y contradictorio que está evolucionando cada vez más rápidamente, en el que el volumen y la multiplicidad de la información convierten a cada individuo, a cada empresa y a cada país en agente y árbitro de un juego que a menudo le supera. Sabemos más y más rápido y sobre más cosas, siendo conscientes, al mismo tiempo, de que la vulnerabilidad está en relación directa con el volumen del flujo de información recabado y de que la realidad virtual a veces gana por la mano a la verdadera.

En una economía globalizada, controlar lo antes posible la información es la clave para poder organizar el mercado y el mundo a voluntad. La capacidad de comprender nuestro entorno con el fin de disponer de la información necesaria para aprovechar las oportunidades que se presenten y evitar los posibles peligros es una disciplina de gestión, es un planteamiento de gestión estratégica.

La economía del conocimiento está llamada a remplazar a la economía tradicional. Mientras tanto, las tecnologías de la información transforman las organizaciones, modifican el entorno en el que se toman las decisiones y dan lugar a nuevas formas de pensar y actuar. El estado actual de conciencia nacional de *ciberseguridad* es, cuando menos, manifiestamente mejorable. Lo cual no es de extrañar dado que el grado de compromiso de la sociedad española con la seguridad y defensa dista mucho de ser óptimo y la *ciberseguridad* es un concepto que ha empezado a llegar al público no especializado hace relativamente poco tiempo.

Para la protección de la seguridad económica de nuestro país, sería necesario considerar a las empresas españolas que proveen tecnologías para la *ciberseguridad* y la inteligencia, por el carácter sensible de sus investigaciones y debido a que las tecnologías desarrolladas son españolas, compañías que deben ser consideradas de interés estratégico de la misma forma que otras son consideradas en otros países, donde se ha creído fundamental posicionarse en este espacio de carácter estratégico.

Entre las funciones que desarrollan estas compañías, se encuentran la de proporcionar información de los riesgos y las amenazas del entorno global actual, ayudando al responsable de la toma de decisiones a vigilar las tendencias y la información susceptibles de afectar a su organización, con el fin de alertarla y advertirla. Una de las soluciones que permiten controlar la sobreabundancia de información consiste en recurrir, por supuesto, a la asimilación del ciclo de información, pero sobre todo a herramientas informáticas de control, monitorización y alerta temprana ante cualquier alerta considerada de interés.

En este sentido, la Estrategia Europea de *Ciberseguridad* ha definido que, para el desarrollo de recursos industriales y tecnológicos para *ciberseguridad*, se promoverá la creación de un mercado único para productos de seguridad. En 2014 se pondrá en marcha un programa para la investigación y desarrollo de tecnologías de seguridad, centrándose en las tecnologías emergentes (se nombra la informática forense y la nube). Además, se incentivará el consumo de productos «seguros» dentro de la UE. Las medidas de incentivación serán el fomento de la gestión del riesgo, adopción de estándares y soluciones de seguridad.

Los procesos de convergencia de la *ciberseguridad, ciberterrorismo, ciberactivismo* y *ciberespionaje,* hacen imprescindible el desarrollo en nuestro país tanto de capacitación personal como de consolidación empresarial de las compañías que realizan servicios en la prevención de todo este tipo de situaciones, tal y como están desarrollando los países de nuestro entorno. Países que se están tomando muy en serio que quien tenga la capacidad de influencia en este quinto espacio será el que detente realmente un principio de soberanía en la toma de sus decisiones como país. Entre las funciones que desarrollan, se encuentran la de proporcionar información de los riesgos y las amenazas del entorno global actual, ayudando al responsable de la toma de decisiones a vigilar las tendencias y la información susceptibles de afectar a su organización, con el fin de alertarla y advertirla. Una de las soluciones que permiten controlar la sobreabundancia de información consiste en recurrir, por supuesto, a la asimilación del ciclo de información, pero sobre todo a herramientas informáticas de control e incluso de traducción.

Para alcanzar una reducción drástica del *cibercrimen*, la UE aboga por endurecer la legislación, desarrollando leyes específicas para «tipos de *cibercrimen*», junto con la creación de alianzas para su persecución. Por las características de los *cibercrímenes*, se requiere disponer de conocimientos especializados y medios tecnológicos para su investigación. Desde la UE se percibe un desequilibrio de capacidades entre los países miembros. Para la eliminación de estas diferencias desde la UE, se financiarán programas dentro de los países miembros para la identificación de fortalezas y carencias en las capacidades para la investigación del *cibercrimen*. De la misma forma, la OSCE, en la reciente reunión sobre nuevas técnicas de investigación contra el crimen organizado y la lucha antiterrorista, aboga por la colaboración y el desarrollo de capacidades tecnológicas y humanas en este sentido. También Europol, a través del EC3 *(European Cybercrime Center)*, desarrolla las capacidades de formación, desarrollo tecnológico e investigación, utilizando la red de Centros de Excelencia en Formación en Ciberseguridad, (ECTEG *European Cybercrime Training & Education Group*) financiados por la Comisión Europea, como el CNEC español, donde está presente el Ministerio del Interior, el Instituto de Ciencias Forenses y de la Seguridad de la UAM y S21sec, como em-

presa privada impulsora del proyecto de colaboración público-privado. El Consejo de Europa, en el Convenio sobre la *Ciberdelincuencia* de Budapest de 2001, manifiesta en su preámbulo la necesaria colaboración en materia penal de los firmantes en la lucha contra la delincuencia informática, considerada una amenaza transnacional.

El *cibercrimen* se ha convertido en uno de los principales problemas para la estabilidad económica de empresas y países. La industria del robo de información para financiar actividades de crimen organizado y terrorismo se ha convertido en un pingüe negocio para las redes de criminalidad organizada. Para defender los intereses legítimos de empresas, ciudadanos y países, algunas empresas se especializan en la recuperación de datos. Este servicio puede convertirse en algo indispensable en un mundo en el que la información interna de la empresa pasa a encontrarse casi totalmente en formato digital.

Una de las dimensiones de la *ciberinteligencia* es la de proteger los activos de la empresa. Ahora bien, estos activos son múltiples y están muy diversificados, hasta el punto de que resulta muy difícil garantizar una cobertura completa. Desde el robo de datos confidenciales contenidos en soporte informático hasta los atentados terroristas contra instalaciones de producción, pasando por la devaluación de la reputación o la imagen de la empresa, los gastos se multiplican cada vez más para las empresas.

Interpol, en su lucha contra el crimen cibernético, declara que:

> *Cybercrime is one of the fastest growing areas of crime. More and more criminals are exploiting the speed, convenience and anonymity that modern technologies offer in order to commit a diverse range of criminal activities. These include attacks against computer data and systems, identity theft, the distribution of child sexual abuse images, Internet auction fraud, the penetration of online financial services, as well as the deployment of viruses, botnets and various email scams such as phishing.*
>
> *The global nature of the Internet has allowed criminals to commit almost any illegal activity anywhere in the world, making it essential for all countries to adapt their domestic offline controls to cover crimes carried out in cyberspace. The use of the Internet by terrorists, particularly for recruitment and the incitement of radicalization, poses a serious threat to national and international security.*
>
> *In addition, the threat of terrorism forces authorities to address security vulnerabilities related to information technology infrastructure such as power plants, electrical grids, information systems and the computer systems of government and major companies.*

La formación, inicial y continua, desempeña por tanto un papel clave en la política pública de *ciberinteligencia*. Para que la iniciativa de *cibersegu-*

ridad traiga como resultado la toma de medidas apropiadas, se requiere formar a especialistas capaces de dirigir políticas de *ciberinteligencia* en las empresas y de elaborar las herramientas correspondientes.

La formación de todos los agentes, por un lado, y de una cantidad adecuada de especialistas, por el otro, supone un avance importante de la enseñanza superior en el plano de la *ciberinteligencia*. Esto se ha de traducir en la constitución de un referente de formación, seleccionando dos ejes de trabajo –la formación inicial y la formación continua– con un objetivo común: lograr que la mayor cantidad posible de responsables de seguridad recurran a la *ciberinteligencia* como método de análisis y de tratamiento de los desafíos, tanto desde la perspectiva de la influencia como de la vigilancia y la protección de los activos.

La voluntad de dotar a España herramientas y métodos óptimos para la práctica de la *ciberseguridad* en los años venideros implicaría numerosas necesidades de investigación en la intersección de las ciencias humanas, lingüísticas, económicas, sociales, políticas y jurídicas, así como de las ciencias y tecnologías de la información y de la comunicación.

Considerar los aspectos claves que configuran una Estrategia Nacional de Seguridad como la recientemente aprobada en España, determinada por su concepción como política de Estado, permite avanzar decididamente en el posicionamiento de nuestro país en el espacio geopolítico internacional. La Estrategia se articula en torno a cinco capítulos en los que se ofrece un concepto de seguridad nacional, se sitúa la seguridad de España en el mundo, se identifican los riesgos y amenazas actuales, se trazan a partir de esta base los objetivos y las líneas de acción estratégicas en los ámbitos de actuación prioritarios para España y se configura un nuevo Sistema de Seguridad Nacional.

Es fundamental considerar que, para garantizar la seguridad de un país, es preciso tener en cuenta el entorno internacional y la competitividad, la *ciberseguridad* y las organizaciones, la gestión de la información y de los conocimientos, la protección y la defensa del patrimonio informático y de los conocimientos, y, finalmente, la influencia y la contrainfluencia.

Los dominios conectados globalmente como el ciberespacio están siendo desafiados de forma creciente por actores tanto estatales como no estatales. Los actores no estatales, como grupos terroristas, traficantes o delincuencia internacional organizada, están interesados en explotar estos dominios, mientras que ciertos estados desarrollan actividades encaminadas a reducir la libertad de movimiento internacional.

Una característica del mercado es la omnipresencia de la información, que constituye una verdadera materia prima estratégica en todos los sentidos. Por este motivo, los desafíos a los que se enfrenta una organización son dos: por un lado, el de recopilar información mediante he-

rramientas especiales, con el fin de contrastarla con otros datos y aprovecharla en el momento oportuno, y, por otro, el de proteger los datos estratégicos de los que dispone.

La economía del conocimiento está llamada a remplazar a la economía tradicional. Mientras tanto, las tecnologías de la información transforman las organizaciones, modifican el entorno en el que se toman las decisiones y dan lugar a nuevas formas de pensar y actuar. Su creciente nivel de importancia ha suscitado desde hace tiempo el interés de organismos internacionales del máximo nivel, como la Organización para la Cooperación y el Desarrollo Económico (OCDE), que considera Internet como un «elemento fundamental para impulsar el desarrollo económico y el bienestar social, así como para fortalecer la capacidad de las sociedades para mejorar la calidad de vida de sus ciudadanos».

A nivel nacional, se debe tratar de establecer un dispositivo de organización flexible y de gran capacidad de reacción, incluso en caso de emergencia, capaz de movilizar los recursos de todos los servicios que lo componen y dotado de los conocimientos y experiencia necesarios para cumplir su tarea con todas las garantías. Incluyendo todas las capacidades de respuesta tanto públicas como privadas.

La aspiración de las empresas a extenderse a mercados extranjeros requiere un proceder metódico y riguroso. La definición del plan estratégico o la elaboración del entramado jurídico y financiero de una operación de exportación o de la creación de una sucursal local exigen una lectura global de la situación geoestratégica y de negocio del país objetivo. El apoyo a las empresas en sus acciones estratégicas genera un círculo virtuoso de evaluación del riesgo y la adopción de las medidas pertinentes para minimizarlo, convirtiendo los riesgos en ventajas competitivas.

Vivimos en un mundo complejo y contradictorio que está evolucionando cada vez más rápidamente, en el que el volumen y la multiplicidad de la información convierten a cada individuo, a cada empresa y a cada Estado en agente y árbitro de un juego que a menudo le supera. Sabemos más y más rápido y sobre más cosas, siendo conscientes, al mismo tiempo, de que la vulnerabilidad está en relación directa con el volumen del flujo de información recabado y de que la realidad virtual a veces gana por la mano a la verdadera.

La decisión de nuestro país, manifestada el día 21 de mayo de 2013 por parte del presidente Rajoy, de dotar a España de un Sistema de Inteligencia Económica supone un hito fundamental en el proceso de concienciación de la necesidad de este modelo de gestión estratégica del país. En palabras del presidente, «facilitará la detección y prevención de actuaciones contrarias a los intereses económicos, financieros, tecnológicos y comerciales de España en sectores estratégicos».

El concepto de sector estratégico se debe someter a una revisión, ya que estratégico tradicionalmente ha estado vinculado con unas compañías de gran tamaño. Este aspecto necesita ser revisado desde el prisma de nuestra capacidad de generar negocio en el exterior, el desarrollo de tecnologías (por ejemplo, la gestión del agua) y el reforzamiento del I+D+i nacional, fomentando una verdadera compra innovadora en nuestra Administración que sirva de elemento tractor para el sector y de influencia en el exterior, reforzando las capacidades comerciales de todos los miembros, no solo de nuestro cuerpo de diplomacia sino de todos los representantes de los distintos ministerios en nuestras delegaciones. Las actividades orientadas a la diplomacia económica y el reforzamiento de nuestra política de I+D en seguridad y *ciberdefensa*, enmarcadas en la actividad del Estado, posibilitan cambios fundamentales en nuestra presencia en los ámbitos internacionales, permitiendo un mayor nivel de acceso a la toma de decisiones en contratos internacionales y fortaleciendo el posicionamiento estratégico no solo de nuestras empresas sino también, por añadidura, de nuestro país.

La capacidad de influencia y contrainfluencia debe estar sustentada en capacidad disuasoria creíble. Para este fin, es necesario contar con un plan estratégico a corto, medio y largo plazo que, a la vez que nos permita tener éxitos inmediatos, genere una cultura de éxito y optimismo que cambie la dinámica de resignación y pesimismo instaurada en nuestra sociedad. La necesidad de éxitos y transmitirlos de la forma adecuada, tanto en el ámbito doméstico como internacional, nos permitirá desarrollar unas acciones de influencia que deben ser consideradas de Estado, independientes de los cambios de gobierno de uno u otro signo.

> *La seguridad nacional es un servicio público objeto de una política de Estado, que, bajo la dirección y liderazgo del presidente del Gobierno, es responsabilidad del Gobierno, implica a todas las Administraciones Públicas y precisa la colaboración de la sociedad en su conjunto.*
>
> *Estrategia Nacional de Seguridad.*

Las conclusiones de nuestro trabajo van en línea con los tiempos. Es necesario un planteamiento de concienciación en materias de *ciberseguridad* de la sociedad civil y de la Administración acerca de los riesgos que les amenazan. La necesaria colaboración de las diferentes Administraciones Públicas y de la sociedad civil es fundamental para la formación de una conciencia nacional de *ciberseguridad.* A pesar de lo doloroso de las crisis, quizás sean estas las que permitan cambios de estructuras que en tiempos de bonanzas se consideran impensables. Las estructuras burocráticas tienden a su perpetuación independientemente de aquellos que las habitan, perviviendo en el tiempo. Las crisis sistémicas proveen el cambio y la evolución: gracias a la crisis indagamos en la salida de ella y nos convertimos en críticos de nuestra forma tradicional de comportamiento.

Para asegurar la resiliencia del ciberespacio, uno de los pilares básicos en la Estrategia Europea de Ciberseguridad, la UE aboga por una legislación y mejora de la concienciación en materia de seguridad. En el ámbito de la legislación, propone la creación de autoridades, a nivel nacional de cada estado miembro, de seguridad de las redes y de la información (sus siglas en inglés NIS). Las entidades a nivel UE ya han sido creadas y tendrán un papel de coordinación, sirviendo de puente entre las diferentes entidades a nivel nacional. Así mismo, la UE estima necesario la regulación de la gestión de los sectores de la energía, transporte, banca, bolsa y proveedores de servicios de Internet desde la perspectiva de hacer una gestión apropiada del riesgo y de informar sobre incidentes de seguridad que impacten en la continuidad de sus servicios esenciales y suministro de bienes. De esta forma, se ha desarrollado en España la Ley 8 /2011 de Protección de Infraestructuras Críticas, la cual, en su preámbulo, recoge la voluntad por parte del legislador de armonizar con la doctrina europea e internacional en esta materia:

> *Los estados modernos se enfrentan actualmente a diferentes desafíos que confieren a la seguridad nacional un carácter cada vez más complejo. Estos nuevos riesgos, generados, en gran medida, por la globalización, y entre los que se cuentan el terrorismo internacional, la proliferación de armas de destrucción masiva o el crimen organizado, se suman a los ya existentes, de los cuales el terrorismo tradicional venía siendo un exponente.*
>
> *En este marco, es cada vez mayor la dependencia que las sociedades tienen del complejo sistema de infraestructuras que dan soporte y posibilitan el normal desenvolvimiento de los sectores productivos, de gestión y de la vida ciudadana en general. Estas infraestructuras suelen ser sumamente interdependientes entre sí, razón por la cual los problemas de seguridad que pueden desencadenarse en cascada a través del propio sistema tienen la posibilidad de ocasionar fallos inesperados y cada vez más graves en los servicios básicos para la población.*
>
> *Hasta tal punto es así, que cualquier interrupción no deseada –incluso de corta duración y debida bien a causas naturales o técnicas, bien a ataques deliberados– podría tener graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, además de provocar perturbaciones y disfunciones graves en materia de seguridad, lo que es objeto de especial atención para el Sistema Nacional de Gestión de Situaciones de Crisis.*
>
> *Dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, que están expuestas a una serie de amenazas. Para su protección, se hace imprescindible, por un lado, catalogar el conjunto de aquellas que prestan servicios esenciales a nuestra*

sociedad y, por otro, diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones... una comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, que contiene propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que les afecten. Con posterioridad, en diciembre de 2004, el Consejo aprobó el PEPIC (Programa Europeo de Protección de Infraestructuras Críticas) y puso en marcha una red de información sobre alertas en infraestructuras críticas (Critical Infrastructures Warning Information Network, CIWIN).

En la actualidad, la entrada en vigor de la Directiva 2008/114 del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE), constituye un importante paso en la cooperación en esta materia en el seno de la Unión. En dicha directiva se establece que la responsabilidad principal y última de proteger las infraestructuras críticas europeas corresponde a los estados miembros y a los operadores de las mismas, y se determina el desarrollo de una serie de obligaciones y de actuaciones por dichos estados que deben incorporarse a las legislaciones nacionales.

Las actuaciones necesarias para optimizar la seguridad de las infraestructuras se enmarcan principalmente en el ámbito de la protección contra agresiones deliberadas y, muy especialmente, contra ataques terroristas, resultando por ello lideradas por el Ministerio del Interior.

Sin embargo, la seguridad de las infraestructuras críticas exige contemplar actuaciones que vayan más allá de la mera protección material contra posibles agresiones o ataques, razón por la cual resulta inevitable implicar a otros órganos de la Administración General del Estado, de las demás Administraciones Públicas, de otros organismos públicos y del sector privado. Estas infraestructuras críticas dependen cada vez más de las tecnologías de la información, tanto para su gestión como para su vinculación con otros sistemas, para lo cual se basan, principalmente, en medios de información y de comunicación de carácter público y abierto. Es preciso contar, por tanto, con la cooperación de todos los actores involucrados en la regulación, planificación y operación de las diferentes infraestructuras que proporcionan los servicios esenciales para la sociedad, sin perjuicio de la coordinación que ejercerá el Ministerio del Interior en colaboración con las comunidades autónomas.

En consecuencia, y dada la complejidad de la materia y su incidencia sobre la seguridad de las personas y sobre el funcionamiento de las

> *estructuras básicas nacionales e internacionales, y en cumplimiento de lo estipulado por la Directiva 2008/114/CE, se hace preciso elaborar una norma cuyo objeto es, por un lado, regular la protección de las infraestructuras críticas contra ataques deliberados de todo tipo (tanto de carácter físico como cibernético) y, por otro lado, la definición de un sistema organizativo de protección de dichas infraestructuras que aglutine a las Administraciones Públicas y entidades privadas afectadas. Como pieza básica de este sistema, la ley crea el Centro Nacional para la Protección de las Infraestructuras Críticas como órgano de asistencia al secretario de Estado de Seguridad en la ejecución de las funciones que se le encomiendan a este como órgano responsable del sistema.*
>
> *La finalidad de esta norma es, por lo tanto, el establecimiento de medidas de protección de las infraestructuras críticas que proporcionen una base adecuada sobre la que se asiente una eficaz coordinación de las Administraciones Públicas y de las entidades y organismos gestores o propietarios de infraestructuras que presten servicios esenciales para la sociedad, con el fin de lograr una mejor seguridad para aquellas. Sobre esta base, se sustentarán el Catálogo Nacional de Infraestructuras Estratégicas (conforme a la comunicación del Consejo de la Unión Europea de 20 de octubre de 2004, que señala que cada sector y cada estado miembro deberá identificar las infraestructuras que son críticas en sus respectivos territorios) y el Plan Nacional de Protección de Infraestructuras Críticas como principales herramientas en la gestión de la seguridad de nuestras infraestructuras.*

En Estados Unidos, el presidente Obama, consciente del riesgo que conllevan los *ciberataques* a las infraestructuras críticas, firmó en febrero de 2013 un decreto con fuerza de ley de *ciberseguridad* que permite al Gobierno compartir información sobre *ciberamenazas* con empresas privadas, específicamente proveedores de infraestructura, haciendo hincapié en la necesidad que tiene el país de enfrentar la amenaza de los *ciberataques*. Obama también llamó al Congreso a aprobar nuevas leyes para darle a nuestro Gobierno una mayor capacidad de asegurar nuestras redes y desalentar los ataques.

> *Sabemos que los hackers roban la identidad de las personas y se infiltran en los correos privados. Sabemos que países extranjeros y empresas roban nuestros secretos corporativos. Ahora nuestros enemigos también están buscando obtener la habilidad de sabotear nuestra red eléctrica, nuestras instituciones financieras y nuestros sistemas de control aéreo. No podemos mirar hacia atrás en el futuro y preguntarnos por qué no hicimos nada ante las amenazas reales a nuestra seguridad y economía.*

La *ciberseguridad* va relacionada inherentemente al riesgo. Por lo que respecta al concepto de riesgo, podemos afirmar que es un constructo social, dinámico y cambiante que requiere para su prevención y miti-

gación de dos herramientas básicas, el conocimiento y la comunicación (información y formación). Es un proceso que permite identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de las amenazas, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse, incluyendo la comprensión que en términos sociales se requiere de la participación de los diversos estratos, sectores de interés y grupos representativos de conductas y modos de vida (incluso de ideologías y de perspectivas del mundo, la vida o la religión) para comprender cómo se construye un riesgo social, colectivo, con la concurrencia de los diversos sectores de una región, sociedad, comunidad o localidad concreta.

En el ámbito de las tecnologías de la información, hace tiempo que se ha asumido la necesidad de convivir con un nivel de riesgo ya que la seguridad total o absoluta no existe. El grado de complejidad de las tecnologías de la información y las comunicaciones ha aumentado considerablemente y cada vez es más difícil administrar el riesgo adecuadamente y, por tanto, controlarlo. En todos estos casos lo que se requiere es revisar el análisis de riesgos del nuevo escenario y tomar rápidamente decisiones correctivas que mitiguen el impacto y permitan salir lo antes posible del escenario de crisis en que nos hemos visto envueltos.

En definitiva, el nuevo enfoque supone, por una parte, realizar los análisis de riesgos entendiendo los ataques posibles (tiempo, capacidad del atacante, progreso del ataque) y, por otra parte, disponer de una capacidad de gestión que pueda informar adecuadamente a los que tienen que tomar decisiones preventivas y reactivas de forma que protejamos no los componentes, sino los servicios finales, sean relativos a la administración electrónica o a los servicios públicos esenciales que, a fin de cuentas, están fuertemente interrelacionados.

Hay que ser sensibles a las responsabilidades, individuales y colectivas, en el campo de la *ciberseguridad*. Las personas poseen una percepción de lo que es la «seguridad ciudadana», de su necesidad y de las implicaciones que una deficiente seguridad ciudadana puede tener para su vida diaria y el ejercicio de sus derechos. Ello viene dado por el conocimiento que poseen sobre las amenazas a esta seguridad, derivadas fundamentalmente de las actividades delictivas más comunes.

Además, en la sociedad de la comunicación en la que vivimos, la alarma social y el estado de opinión pública subsiguiente harían muy difícil para las autoridades la pervivencia de una situación degradada de la seguridad ciudadana. De lo anterior se deduce que es necesario mantener la seguridad ciudadana y que la conciencia de seguridad de la población es importante para mantenerla. Por otra parte, esta conciencia requiere necesariamente del conocimiento de las amenazas a su seguridad por parte de los ciudadanos. La necesidad de crear en el ciudadano una con-

ciencia de *ciberseguridad* es un elemento fundamental de toda estrategia de *ciberseguridad*. Se trata, como se ha dicho anteriormente, de ser conscientes de las amenazas y la complejidad del ciberespacio, así como de asumir las responsabilidades individuales en el campo de la *ciberseguridad*. En resumen, se trata de concienciar al ciudadano para que «habite» el ciberespacio haciendo un uso seguro de las numerosas posibilidades que se le ofrecen.

Si empezamos a nivel nacional, es lógico que el Gobierno se muestre concienciado y sienta la necesidad –y así lo ha mostrado en diferentes ocasiones en los últimos años mediante la publicación de diferentes documentos oficiales sobre política y estrategia de seguridad nacional, en los que hace mención de la seguridad informática– de desarrollar una estrategia nacional de *ciberseguridad* y de fomentar la cultura de *ciberseguridad* y la *ciberurbanidad*. Bajo esta premisa, se desarrolló la Estrategia de Seguridad Nacional de 2011, que sirvió de base para la Estrategia Nacional de Seguridad de mayo de 2013. Pero no es suficiente que el Gobierno esté concienciado, es necesario que todos los altos cargos recogidos en la Ley 5/2006, de 10 de abril, *de regulación de los conflictos de intereses de los miembros del Gobierno y de los altos cargos de la Administración General del Estado* (AGE), y los cargos directamente subordinados a los mismos estén concienciados para que sea factible hacer campañas de concienciación en la AGE susceptibles de tener éxito. La necesidad de comunicación y conocimiento (toma de conciencia) es mayor en los niveles jerárquicos superiores del personal de las Administraciones Públicas, incluido el nivel político, pues la toma de decisiones en relación con la *ciberseguridad* debe tener una buena ubicación para que las prioridades puedan ser adecuadas y el eterno equilibrio entre seguridad y eficacia pueda ser alcanzado.

Derivada de la política de *ciberseguridad*, debe establecerse una estrategia e iniciar campañas de concienciación de *ciberseguridad.* El Spanish Cyber Security Institute (SCSI), en su informe *La ciberseguridad nacional, un compromiso de todos,* deja muy claro que el estado de concienciación en *ciberseguridad* de la sociedad civil es muy bajo, y sobre las campañas desarrolladas por el INTECO, el CCN y el propio SCSI, «de momento, estas iniciativas tienen una repercusión insuficiente en la sociedad civil», y enumera una serie de causas que divide en cuatro grupos: «organizacionales, operacionales, jurídicas y políticas». De entre las causas enumeradas en el citado informe, quiero resaltar las siguientes:

> *Escaso protagonismo de los actores privados en materia de ciberseguridad. La ciberseguridad nacional, hoy en día, es un sistema cerrado y exclusivo de los actores gubernamentales. En la actualidad, más del 80% de las infraestructuras críticas de nuestro país son propiedad, están dirigidas y gestionadas por el sector privado (empresas nacionales e internacionales). Por tanto, la aportación del sector privado al proceso de construcción de la ciberseguridad nacional resulta esencial.*

Ausencia de una política estatal en materia de ciberconcienciación y cibereducación. Muchos países de nuestro entorno están desarrollando ambiciosas políticas en materia de ciberconcienciación y ciberseguridad como eje fundamental para la creación de una cultura de ciberseguridad. Estas políticas han sido desarrolladas e impulsadas, en primera instancia, por el sector privado y, posteriormente, han recibido un fuerte apoyo gubernamental.

En este caso, cabe destacar una doble función, por un lado, concienciar y educar al conjunto de la ciudadanía de los riesgos del ciberespacio y, por otro, identificar futuros talentos en el campo de la ciberseguridad dentro de la comunidad escolar y universitaria.

En España, INTECO y el CCN disponen de programas de ciberconcienciación y ciberseguridad. Desde el sector privado, organismos como el ISMS Forum Spain han lanzado su propia campaña de ciberconcienciación bajo la denominación protegetuinformacion.com. De momento, estas iniciativas tienen una repercusión insuficiente en la sociedad civil.

Ausencia de políticas específicas para el I+D+i nacional en materia de ciberseguridad. No existen políticas, programas o iniciativas para el I+D+i de ámbito nacional que promuevan y faciliten actividades en materia de ciberseguridad, lo que contrasta con el gran protagonismo que a nivel europeo el nuevo marco de trabajo del Horizonte 2020 (continuación del 7.º Programa Marco) otorga a la ciberseguridad.

Las labores de concienciación desarrolladas por las empresas privadas tienen una difusión limitada, empujan a la iniciativa pública, pero es, una vez más, la colaboración público-privada en esta materia es la que puede permitir que no sea un esfuerzo limitado en el tiempo sino que se convierta en una estrategia continuada que vaya íntimamente relacionada con riesgos y amenazas en continuo desarrollo.

En la actualidad, los ciudadanos y muchas empresas tienen intereses que defender frente al *cibercrimen*, fundamentalmente estafas, fraudes, acoso, robo de información, incluida información comprometedora, y similares, pero hay muy poco interés en la defensa colectiva de los intereses de todos. Además, como se ha repetido anteriormente, hay poca conciencia de las amenazas que nos rodean como colectividad en el ciberespacio y menos aún de que podemos ser usados por esas amenazas para encubrirse. Como las amenazas son difíciles de percibir por su propia naturaleza, los ciudadanos tienen dificultades para sentir la necesidad de conciencia de *ciberseguridad.* Sí que pueden percibir algo más la amenaza que supone el *cibercrimen* por su incidencia en su imagen y en su propia economía.

Para desarrollar una conciencia de *ciberseguridad,* es necesario conocer las amenazas y los riesgos y asumirlos, en el sentido de aceptarlos y

enfrentarlos, nunca en el sentido de conformidad y pasividad ante los mismos: comunicar las incidencias, formar en materias de *ciberseguridad* y la necesaria adaptabilidad de usuarios, instituciones y empresas a las circunstancias cambiantes del ciberespacio.

Las escuelas, institutos y universidades juegan un papel primordial en la creación de conciencia de *ciberseguridad*, que será nacional cuando alcance a la mayor parte de la población. Para conseguir la participación de los docentes, es necesario primero concienciarlos y formarlos en *ciberseguridad*, aunque los resultados de la actividad de las instituciones de enseñanza se verán a medio y largo plazo. La conciencia de *ciberseguridad* puede plasmarse en buenas prácticas informáticas o en algo más amplio que podría llamarse *ciberurbanidad* o *cibereducación* y que sería una extensión de las normas y usos de la buena educación al ciberespacio.

Para obtener resultados a corto plazo, es imprescindible que las instituciones de la sociedad civil y los medios de comunicación en todos sus formatos se involucren. Para ello es necesario que los dirigentes de esas instituciones se conciencien de la necesidad de la *ciberseguridad*. En cuanto a los medios de comunicación, los dirigentes tienen un doble papel: concienciarse y concienciar al personal que trabaja en sus medios.

El papel de la sociedad civil es fundamental en la concienciación a corto plazo de todos los ciudadanos y complementa a la obtenida a medio y largo plazo. La necesidad de concienciación ha sido reconocida en la Estrategia Nacional de Seguridad recientemente aprobada, la cual tiene entre sus líneas estratégicas relacionadas con la *ciberseguridad* «la 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».

Los esfuerzos de concienciación deberían seguir haciendo hincapié en la disponibilidad de información clara que pueda ser entendida por todos los participantes y, en especial, por aquellos que carecen o poseen mínimos conocimientos técnicos. Dada la constante naturaleza cambiante del *malware*, las actividades de concienciación deberían ser revisadas o actualizadas regularmente para que siguieran siendo efectivas, lo que ayudaría a mejorar la conducta y prácticas *online* de usuarios así como su capacidad para protegerse de los *ciberataques*.

Los programas de «concienciación» no solo deben concienciar a las personas sino también formarlas y mostrar suficientes casos prácticos en los que se pueda apreciar. Aumentar la concienciación no es un ejercicio único, es un proceso continuo que provoca un cambio cultural que con el tiempo se irá integrando en el día a día del organismo. Para que un programa de concienciación en seguridad tenga éxito, hay dos elementos

clave que son necesarios: la participación de la dirección y el establecimiento de objetivos claros y medibles. Tanto en la empresa privada como en la empresa pública ha de seguirse una línea clara y definida en materias de concienciación y formación.

Los mensajes de concienciación de seguridad necesitan ser adaptados al público objetivo. Para asegurar que los mensajes son relevantes, que se han recibido y entendido, se debe tener en cuenta las particularidades de cada organización y su entorno de trabajo.

El enfoque puede diferir de una organización a otra, pues la forma más eficaz de aumentar la concienciación en una organización dependerá de la cultura de la organización. Llegados a este punto, y sabiendo que el factor humano es siempre el eslabón más débil de la cadena de la seguridad, toca abordar cómo las empresas pueden difundir a lo largo de toda su organización los conceptos de *ciberseguridad* analizados en los apartados anteriores para asegurarse de que los diferentes miembros de la misma disponen del conocimiento adecuado, según su rol y responsabilidad, para asegurar una adecuada conciencia de la situación de la empresa en el ciberespacio que permita a esta garantizar su éxito en este nuevo medio.

Para ello, se debe analizar cómo se puede implantar un programa de concienciación de *ciberseguridad* como herramienta mediante la cual difundir el conocimiento sobre los riesgos de *ciberseguridad* y las posibles contramedidas para paliarlos, para así asegurar la consecución de los objetivos de concienciación citados anteriormente. Una campaña de concienciación orientada a los empleados debe tener presente los diferentes aspectos del problema de la *ciberseguridad.* Aunque cualquier acción es positiva, es realmente necesario que se planifiquen y detallen los objetivos a conseguir.

La concienciación y la formación ayudan a desarrollar una estrecha relación de trabajo entre las áreas y unidades de los organismos y los departamentos TIC, proporcionando un lenguaje y procesos comunes que se pueden utilizar para desarrollar una protección efectiva de los activos de la organización. Aumentar la concienciación es potencialmente la acción más valiosa en la tarea continua de la seguridad. Aumentar la concienciación consigue que todo el personal pertinente tenga suficiente conocimiento de los riesgos y del impacto potencial en el negocio o función de los fallos de seguridad. Los profesionales y los ciudadanos necesitan saber qué hacer para prevenir los ataques y qué hacer en caso de un incidente.

Es esencial que cualquier programa de concienciación de seguridad en un organismo esté correctamente planificado, ya que una sucesión de intentos mal planificados y mal ejecutados pueden obstaculizar los programas de seguridad. Tener un objetivo específico de concienciación centrará los esfuerzos de difusión del mensaje clave en el público apro-

piado y permitirá medir el éxito del programa. Integrar la seguridad en cualquier organización conlleva tiempo y el mejor enfoque es centrarse en los mensajes clave y construir lentamente y en profundidad la concienciación.

En el caso de la seguridad en la Administración Pública, se cuenta con el ENS (Esquema Nacional de Seguridad) que introduce los elementos comunes que han de guiar la actuación en materia de seguridad de las tecnologías de la información. Su finalidad es crear la confianza necesaria en el uso de la administración electrónica por parte de los ciudadanos y permitir el cumplimiento por parte de la Administración de la obligación de prestar acceso electrónico y trámites públicos. En el ENS, se concibe la seguridad como una actividad integral en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

En la Administración Pública española hay comparativamente pocos recursos diseñados específicamente para la formación en seguridad. Los esfuerzos de concienciación deberían seguir haciendo hincapié en la disponibilidad de información clara que pueda ser entendida por todos los participantes y, en especial, por aquellos que carecen o poseen mínimos conocimientos técnicos. Dada la constante naturaleza cambiante del *malware*, las actividades de concienciación deberían ser revisadas o actualizadas regularmente para que siguieran siendo efectivas, lo que ayudaría a mejorar la conducta y prácticas *online* de usuarios así como su capacidad para protegerse de los ataques digitales.

La conciencia de *ciberseguridad* está presente a nivel internacional: todos los países están desarrollando su política de *ciberseguridad* y los organismos internacionales implicados en la seguridad están desarrollando normativas y políticas que permitan afrontar este nuevo escenario donde los desarrollos normativos son escasos y las acciones presentan situaciones no contempladas históricamente. Es comúnmente aceptado que el desarrollo de las tecnologías de la información y las comunicaciones ha hecho del ciberespacio un recurso vital para el desarrollo de la sociedad actual ya que favorece la relación entre personas, empresas y Administración, convirtiéndose en el punto crítico para la prestación de servicios esenciales para el ciudadano.

La necesidad de colaboración entre estados es fundamental ante un aumento del nivel de exposición a sus amenazas y vulnerabilidades. Por tanto, la relevancia de las redes de comunicaciones en el mundo actual lleva asociada, de manera inseparable, la necesidad de protegerlas ante los incidentes de cualquier naturaleza que puedan alterar su operación, ya que las consecuencias de la interrupción o alteración de las redes de

comunicaciones podrían afectar gravemente a funciones sociales fundamentales, tal y como reconoce la recientemente aprobada Estrategia Nacional de Seguridad: «España está expuesta a los *ciberataques,* que no solo generan elevados costes económicos sino también, y lo que es más importante, la pérdida de confianza de los ciudadanos en unos sistemas que, en la actualidad, resultan críticos para el normal funcionamiento de la sociedad».

Esto se ha reflejado a nivel internacional en las correspondientes estrategias nacionales de *ciberseguridad*. El coste estimado del *cibercrimen* a nivel mundial para el 2012 se ha estimado en tres trillones de dólares. Los fenómenos delictivos y de ataque son transnacionales, así que la colaboración entre países para combatir estas amenazas es fundamental. Ataques contra las empresas y contra los países nos hacen replantearnos nuestras políticas de seguridad y defensa; los ataques contra la soberanía nacional de cada país obligan a replantearse los procedimientos de defensa y de respuesta ya que el escenario ha cambiado sensiblemente.

Es necesario desarrollar normas que permitan el respeto a los derechos fundamentales de libertad de expresión y asociación y que protejan el derecho a la propiedad intelectual de empresas, de personas y de Estados; desarrollo de normas que permitan la lucha contra los *ciberdelincuentes*, asegurando el estado de derecho y evitando la creación de santuarios para estos delincuentes. Parece existir una práctica unanimidad a la hora de indicar la necesidad de negociar acuerdos internacionales que regulen el ciberespacio; peor parece la existencia de diferencias insalvables en cuanto a qué deberían incluir esos acuerdos, el carácter de los mismos y las organizaciones de referencia.

Más de una docena de organizaciones internacionales –incluyendo las Naciones Unidas, el G-8, la OTAN, el Consejo de Europa, OSCE, el foro Cooperación Económica Asia-Pacifico, la Organización de los Estados Americanos, la Organización para la Cooperación y el Desarrollo Económicos, la Unión International de Telecomunicaciones (UIT) y la Organización Internacional de Normalización (ISO)– están involucradas en *ciberseguridad*. EE. UU. y Rusia tienen sus propias organizaciones de referencia, el Consejo de Europa y OSCE en el caso norteamericano y Naciones Unidas en el ruso, y ambos se bloquean respectivamente en sus propuestas. En cualquier caso, no debemos perder la esperanza de que las grandes *ciberpotencias* lleguen a un acuerdo que permita fomentar la confianza y aumentar la transparencia reduciendo los crecientes riesgos asociados con los cada vez más numerosos y cada vez más complejos *ciberataques*.

En cualquier caso, se tienen que mantener unos valores esenciales, como es que todo país tiene el derecho a la autodefensa contra actos de agre-

sión en el ciberespacio, autodefensa enfocada en el mantenimiento del funcionamiento de la red global y en la mejora de la *ciberseguridad.*

Otros elementos a tener en cuenta a la hora de redactar normas son: interoperabilidad global, estabilidad de la red y libre flujo de información, acceso fiable a todo individuo y presencia de grupos distintos del Gobierno en la gobernanza de Internet, abierta a actores no gubernamentales.

La *ciberamenaza* se extiende y acrecienta por una falta de normativas internacionales, la dificultad a la hora de atribuir ataques, barreras de acceso débiles y una facilidad relativa para desarrollar capacidades de ataque potentes. Nuestra capacidad de operar en el ciberespacio dependerá de la colaboración entre agencias estatales, no gubernamentales, industria y actores internacionales en el desarrollo de nuevas capacidades, organizaciones y normas, de manera que seamos capaces de proporcionar un amplio abanico de posibilidades para asegurar nuestro propio acceso y uso del dominio del ciberespacio y permitir la persecución de los actores maliciosos. Es necesario mejorar las capacidades de detección, disuasión, bloqueo de acceso y defensa en varias capas (1).

Afirma la OCDE en su informe sobre *Futuros Shocks Globales* (2):

> *A menos que el ritmo de los avances en la ciencia forense cibernética alcance la creciente facilidad de despliegue y la sofisticación de los ciberataques deliberados, seguirá siendo extremadamente difícil para las víctimas conocer la identidad de un atacante –problema de la atribución–. Esto quiere decir que una doctrina de defensa basada en la disuasión es menos probable que tenga éxito, y que ciertas partes malignas que actualmente carecen de la capacidad para poner en marcha un ataque a gran escala con éxito en el futuro pueden hacerlo.*

Otro informe, también publicado por la OCDE, *Reducción del riesgo sistémico en ciberseguridad*, afirma que la cooperación internacional es una de las claves para reducir los riesgos de *ciberseguridad*. Los ataques contra los sistemas conectados a la Internet pública pueden originarse en cualquier parte de esa red. Los fallos en las infraestructuras de información esenciales en una nación pueden transmitirse en cascada en los sistemas dependientes en cualquier parte, pero aunque muchos organismos internacionales han emitido declaraciones de principios de apoyo mutuo y protección, no existe un mecanismo sustantivo de gobernanza internacional para resolver crisis relacionadas con el ciberespacio distintas de la estructura FIRST/CERT dominada por ingenieros (3).

Para establecer una política de ciberespacio coherente a nivel internacional y promover los valores de la UE es necesario continuar trabajando en

la línea de la denominada Convención de Budapest, en la que se acordó la aplicación de las leyes internacionales al ciberespacio. En cuanto a la promoción de los valores de la UE, se apoyará a terceros países en su deseo de dar acceso a las personas a Internet. Además, se hará un seguimiento de aquellos productos que puedan ser utilizados para la vigilancia o censura de forma masiva.

Las principales mejoras que se podrían hacer sería aumentar el número de estados que han ratificado el Convenio sobre la *Ciberdelincuencia* y fortalecer los mecanismos de cooperación internacional y desarrollo de capacidades. Sería particularmente útil que países con un gran número de usuarios de Internet, como Rusia y China, ratifiquen la Convención sobre la *Ciberdelincuencia*. Pero esto puede requerir flexibilidad por parte de los estados parte actuales para responder a las preocupaciones sobre soberanía de Rusia y otros. La OSCE, la mayor organización de seguridad del mundo, ha estado activa en la *ciberseguridad*, principalmente desde la perspectiva de *ciberterrorismo*. En 2010, en un taller OSCE sobre un enfoque global para mejorar la *ciberseguridad,* los delegados coincidieron en que la función de la OSCE en la *ciberseguridad* mundial necesita ser redefinida:

> *Preocupados por la complejidad de las actividades maliciosas en línea, la OSCE ha decidido intensificar la acción mediante la mejora de la cooperación internacional en la lucha contra el uso de Internet con fines terroristas, para considerar la adopción de todas las medidas apropiadas, para proteger las infraestructuras críticas y redes de información vitales contra la amenaza de ciberataques, al considerar ser parte e implementar sus obligaciones en virtud de los instrumentos legales internacionales y regionales existentes; y para explorar la posibilidad de una participación más activa de las instituciones de la sociedad civil y el sector privado en la prevención y lucha contra el uso de Internet con fines terroristas (4).*

Se han definido cinco prioridades en la Estrategia de Ciberseguridad de la UE: conseguir *ciberresiliencia*, reducir drásticamente el crimen organizado, desarrollar una política en *ciberdefensa* y capacidades en materia de seguridad, desarrollar recursos industriales y tecnológicos para *ciberseguridad* y establecer una política de ciberespacio coherente a nivel internacional y promover los valores de la UE.

Así es recogido en el informe del secretario general de la OSCE:

> *Desde 2009, la OSCE ha promovido un enfoque más amplio de la ciberseguridad. Este enfoque se basa en el entendimiento de que el uso generalizado de Internet por los terroristas, traficantes y delincuentes hace cada vez más difícil el desarrollo de respuestas eficaces a las amenazas transnacionales sin promover un ciberespacio más seguro. Un enfoque integral de la ciberseguridad debe: (a) fortalecer la segu-*

ridad nacional; (b) hacer frente a los delitos cibernéticos; (c) inhibir la utilización de Internet por terroristas; (d) responder a una amplia variedad de riesgos y amenazas, incluyendo peligros político-militares; (e) permitir a las autoridades competentes la protección de una amplia gama de objetivos que van desde el usuario particular de Internet a las infraestructuras críticas, y (f) salvaguardar la Internet como un espacio de libre expresión y de reunión.

Uno de los elementos fundamentales de la *ciberseguridad* es la *ciberdefensa.* España acaba de formar el Mando de Ciberdefensa: mediante Orden Ministerial 10/2013, se crea dentro del Estado Mayor de la Defensa el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD). La *ciberdefensa* pasará así a ocupar un lugar importante en la actividad de las Fuerzas Armadas, de forma similar a como ocurre ya en otros países que cuentan con organismos similares, estando a la cabeza de todos ellos el US Cyber Command creado por el Pentágono en 2009 frente a lo que Washington ha definido como el «campo de batalla del futuro».

El ámbito de actuación del MCCD son las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, así como aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la defensa nacional. La misión del MCCD es el planeamiento y la ejecución de las acciones relativas a la *ciberdefensa* militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa nacional. Las funciones serán las siguientes:

- Garantizar el libre acceso al ciberespacio, con el fin de cumplir las misiones y cometidos asignados a las Fuerzas Armadas, mediante el desarrollo y empleo de los medios y procedimientos necesarios.
- Garantizar la disponibilidad, integridad y confidencialidad de la información, así como la integridad y disponibilidad de las redes y sistemas que la manejan y tenga encomendados.
- Garantizar el funcionamiento de los servicios críticos de los sistemas de información y telecomunicaciones de las Fuerzas Armadas en un ambiente degradado debido a incidentes, accidentes o ataques.
- Obtener, analizar y explotar la información sobre *ciberataques* e incidentes en las redes y sistemas de su responsabilidad.
- Ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa nacional.

- Dirigir y coordinar, en materia de *ciberdefensa*, la actividad de los centros de respuesta a incidentes de seguridad de la información de los Ejércitos y el de operaciones de seguridad de la información del Ministerio de Defensa.
- Ejercer la representación del Ministerio de Defensa en materia de ciberdefensa militar en el ámbito nacional e internacional.
- Cooperar, en materia de *ciberdefensa*, con los centros nacionales de respuesta a incidentes de seguridad de la información, de acuerdo con lo que determinen las estrategias y políticas nacionales de *ciberseguridad* en vigor, así como con otros centros militares de respuesta a incidentes de seguridad de la información en el ámbito internacional.
- Definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de *ciberdefensa*.

Se configura la *ciberdefensa* como un elemento fundamental de los intereses del Estado. La necesidad de una conciencia de *ciberdefensa* en España será un trabajo a realizar después del lanzamiento del proyecto a finales del verano. La concienciación en esta materia corresponderá al Mando de Ciberdefensa, así como los planes de capacitación y el desarrollo de las tecnologías a utilizar.

Me gustaría terminar la reflexión volviendo a la Estrategia Nacional de Seguridad recogiendo su primer párrafo del prólogo: «la seguridad es un fundamento esencial para el desarrollo de una sociedad libre», y cito a Félix Arteaga quien, con referencia a la Estrategia, afirma:

> *Las estrategias son documentos con vocación transformadora de las políticas públicas cuya labor comienza –y no termina– con su aprobación, por ello en su valoración se debe diferenciar el contenido de la misma de los mecanismos de puesta en marcha que, a la larga, serán los que demuestren la validez o irrelevancia del documento aprobado. En relación con el contenido, la nueva Estrategia es bastante continuista respecto a la anterior, lo que refleja una vocación de consenso político y de visión de Estado a propósito de la seguridad nacional entre los dos grandes partidos políticos digna de destacar en estos días. Coinciden en identificar como riesgos el terrorismo, los conflictos armados, el crimen organizado, la inseguridad económica y financiera, las «ciberamenazas», los flujos migratorios no controlados, las armas de destrucción masiva, la vulnerabilidad energética y de los servicios e infraestructuras críticas o las emergencias y catástrofes naturales; a los que se añaden ahora el espionaje y la inseguridad marítima. Las coincidencias muestran una visión compartida del contexto estratégico que se prolonga en las líneas estratégicas para afrontar esos riesgos.*

Ambas estrategias comparten una visión integral de la seguridad, transversal, transfronteriza, abierta a nuevos actores públicos y privados para proporcionar la libertad, la seguridad, el bienestar y el funcionamiento de los servicios que precisan los ciudadanos. También comparten la insuficiencia de las estructuras y procedimientos de coordinación existentes para afrontar problemas complejos, por lo que acercan la responsabilidad a la Presidencia del Gobierno:

> *Es desde las más altas instancias del Estado desde donde se pueden marcar las estrategias a seguir y el desarrollo de estas, siendo el modelo de gobernanza un punto clave para su eficaz puesta en funcionamiento. La Agenda Digital para España es un elemento fundamental para desarrollar la confianza en el uso de Internet y de las tecnologías de la comunicación, el desarrollo de las infraestructuras, la inversión en I+D español y su internacionalización, y el desarrollo de una política de compra innovadora desde la Administración.*

Cabe destacar la Estrategia de *Ciberseguridad* Europea aprobada el 7 de Febrero de 2013, basada en cinco principios fundamentales: los valores esenciales de la Unión Europea, que se deben aplicar «tanto en el mundo digital como en el físico», la protección de derechos fundamentales, libertad de expresión, datos personales y privacidad, acceso para todos, gobierno eficiente y democrático de los grupos de interés y responsabilidad compartida.

> *El concepto de seguridad en el siglo XXI debe ser amplio y dinámico para cubrir ámbitos concernientes a la seguridad del Estado y de sus ciudadanos, que son variables según las rápidas evoluciones del entorno estratégico y abarcan desde la defensa del territorio a la estabilidad económica y financiera o la protección de las infraestructuras críticas.*
>
> *Por otra parte, la respuesta a los riesgos y amenazas que comprometen la seguridad en nuestros días precisa de cooperación tanto en el plano nacional como en el multilateral. Las respuestas unilaterales y aisladas no son eficaces, por su carácter incompleto y parcial, frente a unos retos que exigen un enfoque multidisciplinar y una acción conjunta. Solo esta perspectiva abarca todos los aspectos potencial o realmente afectados.*
>
> *Los cambios y tendencias relativos al entorno de la seguridad, sus dimensiones y las respuestas que pide su preservación son factores que inciden en la visión de la seguridad nacional. España se sitúa junto a los países más avanzados en la materia y concibe la seguridad de una manera integral, acorde con las transformaciones globales que repercuten en el Estado y la vida diaria del ciudadano. En esta línea, la crisis financiera y económica que actualmente afecta a España, a la zona euro y a parte importante de las economías mundiales represen-*

ta uno de los mayores retos para la seguridad nacional y extrema la necesidad de ser eficientes en la respuesta.

Estrategia Nacional de Seguridad

Una política de Estado no solo debe ser abordada desde los poderes públicos; es fundamental, y en este caso de forma particular, colaborar con el sector privado en el entendimiento y el desarrollo de esta política que nos afecta a todos, puesto que la seguridad es una tarea compartida. El desarrollo de la Estrategia Nacional de Ciberseguridad necesitará de la implantación de una cultura de *ciberseguridad* sólida, concienciando a los ciudadanos, a las empresas y a la Administración 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. Del mismo modo, siguiendo la política de *ciberseguridad* de la UE, se fomentará el desarrollo de tecnologías nacionales a través de un programa de I+D, así como la capacitación de profesionales en estas materias.

Bibliografía

1. *Estrategia Nacional Militar de los Estados Unidos de América.* Washington, EE. UU.: Joint Chief of Staff, 2011.
2. OCDE. *Future Global Shocks. Improving Risk Governance.* París: OCDE, 2011.
3. SOMMER, Peter y BROWN, Ian. *Reducing Systemic Cybersecurity Risk*. Informe OCDE, 2011.
4. OSCE_MC.DEC/7/06. *Decision No. 7/06. Countering the Use of the Internet for Terrorist Purposes.* Bruselas: OSCE, 2006.
5. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Bruselas: European Commission & High Representative of the European Union for Foreign Affairs And Security Policy, 2013.
6. KAGAN, Robert. *Paradise and Power: America and Europe in the New World Order.* Londres: Atlantic Books, 2004.
7. WEGENER, Henning. *Regulating Cyber Behavior: Some Initial Reflections on Codes of Conduct and Confidence Building Measures.* [En línea] 23 de agosto de 2012 [citado el 29 de marzo de 2013]. http://www.federationofscientists.org/PlanetaryEmergencies/Seminars/45th/Wegener publication.docx.
8. BAILEY, Eric. *«Nothing Can Justify Torture»: An interview with Noam Chomsky on Obama's Human Rights Record.* [En línea] 12 de diciembre de 2012 [citado el 30 de marzo de 2013]. http://chomsky.info/interviews/20121212.htm.
9. *Cyberspace Policy Review.* Washington: The White House, 2011. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

10. *International Strategy for Cyberspace.* Washington: The White House, 2011.
11. BIDEN, Joseph R. *VP's remarks to London Cyberspace Conference.* Londres: The White House, 2011.
12. CLAPPER, James R. *Worldwide Threat Assessment of the US Intelligence Community 2013.* Washington D. C.: Office of the Director of National Intelligence, 12 de marzo de 2013.
13. ALEXANDER, Keith B. *Statement of general Keith B. Alexander Commander United States Cyber Command before the Senate Committee on Armed Services.* Washington: United States Cyber Command, 2013.
14. PELLERIN, Cheryl. American Forces Press Service. Cybercom Builds Teams for Offense, Defense in Cyberspace. [En línea] 12 de marzo de 2013 [citado el 30 de marzo de 2013]. http://www.defense.gov/news/newsarticle.aspx?id=119506.
15. KEHLER, C. R. *Statement of general C. R. Kehler Commander United States Strategic Command before the Senate Committee on Armed Services.* Washington: United States Strategic Command, 12 de marzo de 2013.
16. LEWIS, James Andrew. *Critical Questions for 2013: Global Challenges. What's Next in Cybersecurity?* [En línea] 25 de enero de 2013 [citado el: 30 de marzo de 2013]. Center for Strategic and International Studies. http://csis.org/publication/critical-questions-2013-global-challenges.
17. BUMILLER, Elisabeth. «Pentagon to Beef Up Cybersecurity Force to Counter Attacks», *The New York Times*. [En línea] 29 de marzo de 2013 [citado el 31 de marzo de 2013]. www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html.
18. GEERS, Kenneth. *Cyberspace and the changing nature of warfare.* [En línea] 27 de agosto de 2008 [citado el: 31 de marzo de 2013]. http://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/.
19. HEALEY, Jason y VAN BOCHOVEN, Leendert. *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow.* Washington: The Atlantic Council of the United States, 2011.
20. PRINCE, Matthew. «The DDoS That Almost Broke the Internet». [En línea] 27 de marzo de 2013 [citado el 28 de marzo de 2013]. *Cloud Flare.* http://blog.cloudflare.com/the-ddos-that-almost-broke-the-Internet.
21. TIKK, Eneken. *Comprehensive legal approach to cyber security 2011.* Tarfu, Estonia: Faculty of Law, University of Tartu, 2011.
22. Council Framework Decision 2005/222/JHA. *Official Journal of the European Union.* [En línea] 16 de marzo de 2005 [citado el 31 de mar-

zo de 2013]. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf.

23. FROOMKIN, Michael. «Cybercrime Treaty Goes Live». *Discourse.net.* [En línea] 19 de marzo de 2004 [citado el 31 de marzo de 2013]. http://www.discourse.net/archives/2004/03/cybercrime_treaty_goes_live.html.
24. ARCHICK, Kristin. *CRS Report for Congress. Cybercrime: The Council of Europe Convention.* Washington: Congressional Research Service, 2004.
25. SCHJØLBERG, Stein y GHERNAOUTI-HÉLIE, Solange. *A Global Protocol on Cybersecurity and Cybercrime: An Initiative for peace and Security in Cyberspace,* segunda edición. Oslo: AiTOslo, 2011.
26. [En línea] 16 de octubre de 2009 [citado el 31 de marzo de 2013]. EE. UU.: OSCE, 2013. https://dazzlepod.com/cable/09STATE107552/.
27. SCHNEIDER, Deborah. *United States Mission to the OSCE Cyber Security Keynote Address by Dr. Deborah Schneider, U. S. Department of State as delivered to the Joint FSC/PC.* Viena: OSCE, 2010.
28. SAFIRE, William. «The Farewell Dossier». *The New York Times.* [En línea] 2 de Febrero de 2004 [citado el 2 de enero de 2013]. http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?ref=williamsaire.
29. BROWN, Gary y POELLET, Keira. «The Customary International Law of Cyberspace», IV, 2012. *Strategic Studies Quarterly,* otoño de 2012, vol. 6, págs. 126-145.
30. STEPHENS, Bret. «The Limits of Stuxnet». *The Wall Street Journal.* [En línea] 18 de enero de 2011 [citado el 2 de enero de 2013]. http://online.wsj.com/article/SB10001424052748703396604576087632882247372.html.
31. PERTERMANN, Kerstin. *Conference Report: Challenges in Cybersecurity, Risks, Strategies, and Confidence-Building International Conference.* Hamburgo: Institute for Peace Research and Security Policy at the University of Hamburg, 2011.
32. VENTRE, Daniel. *La politique de cyberdéfense peut-elle être a-politique?* Paris: Ministère de la défense Délégation aux Affaires Stratégiques, 2013.
33. OBAMA, Barak. *Discurso sobre el estado de la Unión de Barack Obama.* Washington: The White House, 2013.
34. NEWMEYER, Kevin P. *Who should lead U.S. Cyber security efforts? PRISM*, 2012, vol. 3, n.º 2, págs. 115-126.
35. *Estrategia Española de Seguridad.* Madrid: Gobierno de España, 2011.
36. PÉREZ, Jesús. «Cómo Cyberbunker atacó a Spamhaus y casi se llevó a medio Internet por delante». *Security by Default.* [En línea] 28 de

marzo de 2013 [citado el 12 de mayo de 2013]. http://www.security-bydefault.com/2013/03/como-cyberbunker-ataco-spamhaus-y-casi.html.

37. VENTRE, Daniel. «Japon: stratégies de cyberdéfense, Multi-System and Internet-Security-Cookbook». *MISC,* 2012, n° 64, págs. 65-73.
38. BAGCHI, Sohini. «India needs more warriors in the cyber space». *Cxotoday.com.* [En línea] 3 de mayo de 2013 [citado el 12 de mayo de 2013]. http://www.cxotoday.com/story/india-needs-more-warriors-in-the-cyber-space/.
39. ZORZ, Zeljka. «India has a new National Cyber Security Policy». *Help net security organization.* [En línea] 10 de mayo de 2013 [citado el 12 de mayo de 2013]. http://www.net-security.org/secworld.php?id=14891.
40. FEDORENKO, Andrei. «The Fight Over the Draft. UN Convention on International Information Security». *Regulatory cyber security: The FISMA focus IPD.* [En línea] 15 de julio de 2012 [citado el 12 de mayo de 2013]. http://www.thecre.com/fisma/?p=2173.
41. *Information systems defence and security - France's strategy*. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), 2011.