INTERVENCIÓN DEL SECRETARIO DE ESTADO DE SEGURIDAD, FRANCISCO MARTÍNEZ, EN LA CLAUSURA DE LAS JORNADAS SOBRE EL IMPACTO DE LA CIBERSEGURIDAD EN LOS NEGOCIOS

Madrid, 25 de septiembre de 2013

Quiero agradecer a la escuela de negocios Next y a la empresa de ciberseguridad S21sec, representadas ambas por quienes me acompañan en la mesa, no tanto que me hayan invitado a clausurar este evento, algo que sin duda les agradezco, sino sobre todo por que se tomen la molestia y el esfuerzo de organizar Jornadas como estas. Es preciso indagar en realidades nuevas, como la ciberseguridad, que son el pan nuestro de cada día, que están presentes en todos nuestros actos cotidianos aunque no siempre sean perceptibles. El ciberespacio es esa tupida red que se teje a nuestro alrededor cuando mandamos una foto con el móvil o cuando pagamos una entrada de cine con la tablet.

Pero dejemos que nos hable del ciberespacio el gran Ortega y Gasset. Ya lo sé, me miran extrañados porque, cuando murió en esta ciudad de Madrid en 1957, no había nada que se pareciese a Internet o el ciberespacio. Pero José Ortega y Gasset hace una reflexión sobre la ciudad que nos puede servir para entender qué es eso que llamamos ciberespacio. Una vez comprendida la estructura de ese espacio cibernético, podemos pensar cuál es la seguridad que necesita. Por último, y entonces estará justificada mi presencia hoy aquí, podremos hablar de cuál es el rol del Estado en la provisión de seguridad en el ciberespacio, entender qué es eso que podríamos llamar ciberseguridad pública.

Pero vayamos por pasos. Primero Ortega. La cita es un poco larga, pero no tiene desperdicio. Decía el filósofo madrileño: «Ciudad es ante todo plaza, ágora, discusión, elocuencia. De hecho, no necesita tener casas, la ciudad; las fachadas bastan. Las ciudades clásicas están basadas en un instinto opuesto al doméstico. La gente construye la casa para vivir en ella y la gente funda la ciudad para salir de la casa y encontrarse con otros que también han salido de la suya.»

¿No les recuerda esta descripción a lo que ocurre en el ciberespacio? ¿No concuerda esta ciudad orteguiana, sin paredes ni divisiones, con la realidad de un ciberespacio que es punto de encuentro?

El ciberespacio es punto de encuentro entre personas. Disuelve distancias de miles de kilómetros para permitir una comunicación directa entre individuos. Permite también la interconexión entre empresas o entre empresas y consumidores. Las rígidas estructuras de la fábrica y los sólidos muros de las corporaciones se desmoronan gracias a un ciberespacio en el que los productos llegan a consumidores lejanos, pero en el que estos consumidores se vengan, por así decirlo, haciendo llegar sus ideas y preferencias a los que producen y diseñan productos o servicios. A través de las redes sociales el usuario pasa a formar parte del equipo de producción o de marketing, entra en el consejo de dirección.

Se diría que en el ciberespacio se desmoronan los muros de las empresas y, tal como decía Ortega, sólo quedan las fachadas. El mundo entero, gracias a una comunicación fácil, inmediata y universal, se convierte, como decía también el filósofo, en plaza, ágora, discusión, elocuencia.

Antes de pasar a hablar de los riesgos de seguridad en este ciberespacio y de las medidas a adoptar, vamos a tratar de pensar cómo se ha producido este milagro de la ciudad virtual que nos ha dejado con una ciudad en la que no hay muros, sólo fachadas, y las plazas que están repletas de gente que habla y comercia, que dialoga e intercambia.

Me permitirán que siga el ejemplo de Ortega, alguien que creía que no hace falta recurrir al alemán, al francés o al inglés para pensar, sabía que lo que un español debe hacer es pensar en su idioma. Parece casi imposible pensar solo en español en un ámbito como este, en el que a cada paso nos aguarda un vocablo inglés. Pero probemos.

En un lugar como este, Ilustre Colegio de Ingenieros Industriales de Madrid, es de justicia mencionar que el ciberespacio se sustenta sobre tres palabras que deben mucho al ingenio de ingenieros, matemáticos y físicos. Estas tres palabras son informática, computación y redes.

Las redes son esa maraña de cables de cobre, fibra óptica, antenas y repetidores, espacios wifi o satélites que hacen posible el primer milagro del ciberespacio: contraer el espacio físico hasta hacer del mundo entero una sola plaza. En eso consiste el ciberespacio: en la reducción del vasto mundo a un pequeño lugar, en achicar distancias para facilitar la comunicación.

Pero queda otra restricción, junto a la del espacio, a la que siempre estamos sometidos los humanos: el tiempo. A paliar y aminorar la falta de tiempo nos ayudan esas máquinas sobre las que se sustenta internet y el ciberespacio: los ordenadores o computadoras, que es como prefieren llamarlas en español nuestros hermanos de América Latina.

¿Cómo ayudan las computadoras a comprimir el tiempo? Pues computando. Somos capaces hoy día de predecir el tiempo porque, además de buenos modelos matemáticos, disponemos de supercomputadoras que hacen en segundos los cálculos que a un meteorólogo le llevaría años con papel y lápiz. Miles de aviones aterrizan en nuestros aeropuertos cada día ayudados por complejos sistemas de navegación que asisten en el despegue y el aterrizaje. Con la sola capacidad humana, una pizarra y una tiza, dudo mucho que pudiera aterrizar más de un avión cada cinco minutos. Así pues, las computadoras operan el milagro de comprimir el tiempo, de hacer, cual fieles esclavas, las tareas que llevarían milenios a cualquier hombre.

Pero los milagros de la contracción del espacio y el tiempo no valdrían de nada si lo que se mueve en ese espacio-tiempo comprimido no tuviese valor. La clave nos la dará la última palabra por analizar: informática, o más bien, la palabra a la que ésta remite: información.

Lo que se intercambia en dispositivos móviles, lo que se almacena con sumo cuidado en servidores o en la nube, con lo que en última instancia se comercia en la red es con información. Un hombre le dice a otro hombre algo. Ese simple acto está a la base de todo lo que ocurre en el ciberespacio. Es ese hecho sobre el que Ortega nos llama la atención: “la gente construye la casa para vivir en ella”, pero “la gente funda la ciudad para salir de la casa y encontrarse con otros que también han salido de la suya”.

Esa es la clave de todo el ciberespacio, por encima de toda la complejidad de cables, espacios radioeléctricos y ordenadores, hay un acto de comunicación, de intercambio de información, de hombres hablando a otros hombres.

Ahora aparece con claridad lo que queremos proteger en el ciberespacio. Por un lado es preciso salvaguardar la intimidad y privacidad que las personas buscan en su comunicación con otras personas. Y en este sentido, la lucha en favor de una mayor ciberseguridad se realiza contra los que se introducen en ordenadores o dispositivos ajenos para acceder a

su información, ya sea por motivos económicos, para chantajear o para denigrar la integridad personal o sexual de alguien.

Por otro lado, la seguridad en la web, en ese ciberespacio, es la seguridad de la plaza pública, del mercado. Según un estudio del Ministerio de Industria, Energía y Turismo el 66,3% de los internautas compraron en 2011 a través de Internet. Según el último informe de la CMT, la Comisión del Mercado de las Comunicaciones, en el primer trimestre de 2013 el comercio electrónico en España alcanzó un volumen de negocio de 2.822 millones de euros, un 15,1% más que en el mismo trimestre de 2012. Se realizaron un total de 43,5 millones de operaciones.

Ese mercado, porque está sometido a las amenazas del crimen, necesita una protección legal y efectiva.

Según estimaciones del Department of Homeland Security de los Estados Unidos en el ciberespacio confluyen cada día más de 2 mil millones de personas y hasta 8 mil millones de aparatos, desde ordenadores, móviles, GPs, etc. Parece obvio que ese espacio, en el que además se realizan millones de transacciones comerciales cada hora, deba estar sometido a la legalidad y a un cierto orden. ¿Pero cuál debe ser el papel del Estado?

Me permitirán dos breves disgresiones etimológicas. Es curioso que el prefijo ciber venga del griego cybernetikós, que se traduce literalmente como gubernamental. Así que algo tendrá que ver el Gobierno con lo cibernético, aunque quien puso el nombre pensara más bien en la palabra gobierno como quien gobierna o guía un barco para navegar por la red.

La otra etimología es más conocida. Policía tiene su origen en pólis, la ciudad griega, ese lugar en el que confluyen las personas para hablar y discutir. También en la nueva ciudad virtual que conforma el ciberespacio hay un papel para los que mantienen el orden y hacen respetar la ley, por la policía.

Pues bien, la Constitución Española, al igual que todas las Constituciones, encomienda al Estado, asistido por las Fuerzas y Cuerpos de Seguridad, la salvaguardia de la integridad física de los ciudadanos y de sus bienes. El mandato constitucional encarga a las fuerzas policiales proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana. Este mandato se extiende, claro está, también al ciberespacio.

Es necesario adoptar medidas de seguridad porque existen riesgos reales. ¿Cuáles son esos riesgos que amenazan las redes físicas, la información y el bienestar de los usuarios a través del ciberespacio?

Actualmente, después de la prostitución y el tráfico de drogas, el delito más lucrativo a nivel mundial es el cibercrimen. En el espacio virtual tienen cabida prácticamente todos los delitos desde la pornografía infantil y los timos tradicionales, hasta los ataques terroristas o criminales a sistemas de información y las estafas más sofisticadas desde el punto de vista tecnológico.

Según la Administración de Estados Unidos, en 2012 las pérdidas originadas en el cibercrimen equivalían al 1,75% del PIB mundial, unos 1,3 billones de dólares, una cantidad similar al PIB de España.

Ante los riesgos securitarios en el ciberespacio es preciso adoptar una batería de acciones que resumiré en cuatro: primero, capacidad de prevención, detección y respuesta; segundo, lucha contra el ciberterrorismo y protección de las infraestructuras críticas; tercero, lucha contra el cibercrimen; y cuarto, la protección en la red de los grupos más vulnerables.

Una vez acabe de hablar de estos cuatro campos de la ciberseguridad, concluiré mi intervención mencionando a los socios con los que las instituciones públicas deben trabajar en pos de una mayor ciberseguridad, pero les adelanto que son tres: otros Estados, el sector privado y los ciudadanos.

Para tratar de la prevención, detección y respuesta volveré a citar a Ortega y Gasset cuando dice que “el río se abre cauce y luego el cauce esclaviza al río”. ¿Qué quiere decir esta bella frase en el contexto de la ciberseguridad?

Pues que al igual que las capacidades tecnológicas han abierto un cauce por el que fluye comunicación e información, esa comunicación e información están contenidas en ese cauce que forman las redes de telecomunicaciones e informáticas. Desde el punto de vista policial esto tiene una gran ventaja. Sabemos dónde se va a cometer el delito: en el cauce de ese río con mil brazos que se llama Internet.

El río es inmenso, pero tiene cauces definidos, así que resulta posible prevenir en él los ataques cibercriminales o ciberterroristas, detectarlos en ese cauce y luego responder a la amenaza.

Dado que gran parte de la vida social y económica de nuestros tiempos se desarrolla en el ciberespacio o está expuesta a lo que en él ocurre, es especialmente importante prevenir amenazas, detectar de dónde provienen y darles una respuesta adecuada que sirva de castigo y disuasión futura.

Para ello, las Administraciones Públicas españolas se han dotado de distintos CERTs (Computer Emergency Readiness Teams o Equipos de Respuesta para Emergencias Informáticas). Hay que destacar cuatro CERTs: en primer lugar, el del Centro Criptológio Nacional, dependiente del CNI, que da respuesta nacional a las amenazas que afecten a las administraciones públicas o empresas estratégicas; en segundo, el del INTECO en el Ministerio Industria, especialmente orientado a asistir a empresas y ciudadanos; en tercero, asistiendo a nuestras Fuerzas Armadas, el CERT-FAS; y por último, CNPIC, o Centro Nacional de Protección de Infraestructuras Críticas, dependiente de la Secretaría de Estado de Seguridad.

Por ser este Centro de mi directa competencia les hablaré más en extenso de él.

Dije antes que uno de los campos de acción de la ciberseguridad es la lucha contra el ciberterrorismo. El ciberespacio se ha convertido en un nuevo campo de batalla para la acción terrorista contra los Estados. Los grupos terroristas utilizan las redes digitales para atacar objetivos estratégicos o infraestructuras críticas.

Estas, las infraestructuras críticas, son aquellas que aseguran servicios esenciales para la economía y el desarrollo social de nuestro país. Aeropuertos, puertos, transporte ferroviario o por carretera, suministros de electricidad o agua, centrales nucleares y pantanos, todos están conectados a las redes digitales para su control y operatividad. Por ello, a través de estas redes digitales, son vulnerables a ataques de ciberterrorismo.

A través de las redes digitales una red terrorista desde ordenadores remotos podría parar los sistemas de refrigeración de una central nuclear, causando una catástrofe humana y medioambiental. Por los aeropuertos

españoles cada año transitan 200 millones de personas. El control del tráfico aéreo depende de redes informáticas que es preciso proteger contra ataques terroristas de potenciales terribles consecuencias.

Es de vital importancia para la seguridad de cualquier país aumentar la resiliencia de sus infraestructuras críticas para evitar una potencial alteración del funcionamiento normal de servicios esenciales.

Para incrementar, pues, la resiliencia de nuestros sistemas críticos, la Secretaría de Estado de Seguridad se ha dotado del Centro Nacional de Protección de Infraestructuras Críticas, el CNPIC, que trabaja en estrecha colaboración con los operadores de tales infraestructuras, en su mayoría agentes privados, para desarrollar programas que fortalezcan la seguridad tanto en el ámbito físico como en el tecnológico.

Quiero, además, mencionar la colaboración interministerial en este ámbito entre el Ministerio del Interior y el de Industria, Energía y Turismo. A principios de 2013, la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información firmamos un Convenio marco de colaboración en materia de ciberseguridad. El objetivo del convenio es:

- por una parte, desarrollar un marco de seguridad en la red, minimizando los riesgos
- y por otra, fomentar que el ciberespacio sea un entorno donde las redes y los sistemas de información posibiliten el desarrollo de la actividad industrial, empresarial, tanto pública como privada.

Pasemos a hablar de la ciberdelincuencia. Para la lucha contra el crimen organizado en la red España cuenta con equipos especializados y personal altamente cualificado de la Guardia Civil y del Cuerpo Nacional de Policía.

El ciberespacio se ha convertido en un nuevo y prometedor medio para el crimen organizado. Los ciberdelincuentes se distribuyen las tareas de forma que unos crean el malware y otros se encargan de la recogida de dinero (estructura de “mulas”). La Delincuencia Organizada está asimismo detrás de actividades de robo de datos bancarios, financieros y personales.

Como ejemplo de la lucha contra este tipo de delincuencia les daré el de la operación “Ramson”. Los delincuentes infectaban el ordenador de un usuario y lo bloqueaban, solicitando para su desbloqueo el pago electrónico de 100€. Fue una gran operación contra una organización que

actuaba no solo en España, sino en diversos países europeos y americanos.

Los ataques están destinados en ocasiones a robar datos o perjudicar los servicios de una empresa de la competencia. Este año la policía española, en colaboración con el FBI y la policía holandesa, detuvo en España al responsable del mayor ataque cibernético de denegación de servicio de la historia.

Por último, en el campo de la cibereincuencia no hay que olvidarse del espionaje industrial. Es una amenaza real y de enorme trascendencia económica y estratégica. En la era del conocimiento el principal activo de las empresas es su know-how, su I+D o sus bases de datos. La sustracción de esta información para ser vendida a la competencia es un serio riesgo para las empresas industriales y financieras. Estoy seguro de que en las distintas ponencias que han tenido lugar hoy se ha hablado con profusión de las respuestas que las empresas de seguridad aportan en este campo.

Hay una última función que compete muy especialmente al Estado en la provisión de eso que podríamos llamar ciberseguridad pública. Se trata de proteger a los grupos más vulnerables en la red. Además una lucha continua y creciente contra la pornografía infantil, la policía y la guardia civil reciben numerosas demandas o quejas por grooming (acoso sexual), cyberbulling (acoso y vejación), captación de menores por parte de pederastas en las redes sociales, publicación incontrolada de datos personales, etc.

La labor de las Fuerzas y Cuerpos de Seguridad en este ámbito cobran un especial valor para toda nuestra sociedad.

Pero las instituciones públicas españolas, por muchos medios humanos y técnicos, por muchos esfuerzos que le dediquen a la lucha contra la inseguridad en el ciberespacio, no pueden tener éxito si actúan solas. Es imprescindible el concurso de al menos tres grupos en esta lucha contra los que quieren aprovecharse de la cercanía e inmediatez que proporciona la red.

El primero es la comunidad internacional. No es suficiente lo que hagamos desde España. Ante amenazas de carácter internacional en un ciberespacio global, es imprescindible reforzar la cooperación internacional.

En el ámbito policial es especialmente fructífera la colaboración con Interpol y Europol. Concretamente, en lo que tiene que ver con la ciberseguridad, Europol ha puesto en funcionamiento el European Cybercrime Centre, conocido como EC3, que permite coordinar mejor la lucha europea contra la delincuencia en la red.

España tiene un firme y largo compromiso con la seguridad internacional, compromiso que se extiende a la seguridad del ciberespacio. Nuestro país está y estará presente en los foros internacionales en los que se discuten las estrategias y medidas de ciberseguridad; en los foros europeos en los que se armoniza la legislación que afectará la seguridad del ciberespacio europeo; y España, a través de distintos organismos como Naciones Unidas, la OTAN, la OSCE o la OCDE, impulsa canales internacionales para compartir tanto información como esfuerzos de prevención y respuesta ante las amenazas contra la ciberseguridad.

Las redes digitales están mayoritariamente en manos de empresas privadas, por lo que me temo que tendré que decir una obviedad: la ciberseguridad sólo se puede conseguir de manera efectiva reforzando la colaboración público-privada entre las administraciones y los sectores industriales, particularmente los de las tecnologías de la información y las telecomunicaciones.

Pero esa colaboración no debe ser la de un sector público que viene a imponer normas rígidas a un sector dinámico en el que la innovación es esencial y la continua transformación es lo que lo mantiene con vida. No se trata de imponer regulaciones para congelar el ciberespacio y que así sea más manejable. Eso lo destruiría.

La colaboración público-privada tiene que ver más con encontrar juntos soluciones tecnológicas y canales de cooperación. Por dar un ejemplo: las investigaciones en criptografía las llevan a cabo tanto servicios de inteligencia de los distintos países, como empresas privadas de seguridad, así como universidades.

Las soluciones innovadoras y duraderas de ciberseguridad son fruto de una estrecha colaboración entre universidades, centros de investigación, empresas y el sector público. En la carrera hacia la adquisición de nuevas tecnologías España no se puede quedar atrás. No nos jugamos solamente la independencia tecnológica en las soluciones de ciberseguridad, sino también el poder o no participar en un mercado de peso creciente y gran potencial.

Más allá de la colaboración con nuestros socios europeos o americanos, España debe también desarrollar tecnologías propias en el ámbito de la ciberseguridad. Es imprescindible, pues, apostar por la investigación y el desarrollo, y eso, en tiempos de escasez de fondos, pasa por partenariados público-privados.

Apoyar a las empresas españolas de ciberseguridad que invierten en I+D es una cuestión estratégica. El apoyo no sólo es cuestión de financiar programas o proyectos, algo que quizás presupuestariamente sea difícil en estos momentos. Es preciso apoyar a las empresas con una normativa favorable, en asuntos como las certificaciones de tecnologías y procedimientos ciberseguros. También se ha de apoyar al sector de la ciberseguridad ayudándole en la internacionalización.

La alternativa es que nuestras empresas sean compradas por competidores extranjeros y estar condenados a una interminable dependencia tecnológica.

Y para concluir hablaré de la necesidad de fomentar una cultura de la ciberseguridad: hacer a los ciudadanos corresponsables de su propia seguridad también en el ciberespacio. Esta búsqueda de la complicidad y la colaboración de los ciudadanos en la ciberseguridad será en el medio y largo plazo la mejor herramienta para lograr una seguridad reforzada de todos los ciudadanos.

Hay que impulsar actividades de sensibilización sobre los riesgos en el ciberespacio, para que ciudadanos y empresas conozcan las amenazas, las vulnerabilidades y puedan tomar medidas para mejor protegerse.

Las PYMES precisan de mecanismos de apoyo para reforzar el uso seguro que hacen de las tecnologías de la información y las comunicaciones.

Por su parte la educación de los menores en los riesgos del ciberacoso o de abuso sexual en la red resulta imprescindible para proteger a este grupo vulnerable.

Tal como dice explícitamente la recién publicada Estrategia de Seguridad Nacional: “Garantizar la seguridad es una responsabilidad del Gobierno, pero es también una tarea de todos”.

Y como no hay dos sin tres, acabaré con una tercera cita de Ortega. Decía el más claro de nuestros pensadores que “los hombres no viven juntos porque sí, sino para acometer juntos grandes empresas”. A los hombres a los que nos ha tocado vivir este siglo XXI en el que repartimos nuestra vida entre el mundo físico y el ciberespacio, en el que vivimos vidas reales y virtuales, nos toca acometer juntos el reto de que esta nueva ciudad en la que no quedan muros y tan solo fachadas, en la que los hombres están cerca incluso de los que están lejos, nos toca afrontar el reto, decía, de que esta nueva ciudad del ciberespacio sea segura, próspera y libre.

Muchas gracias.