INTERVENCIÓN DEL MINISTRO DEL INTERIOR EN LAS JORNADAS UNIVERSITARIAS DE LOS PIRINEOS "DESCUBRIR LA IDENTIDAD HUMANA EN UN MUNDO DIGITAL"

"LOS RETOS DE LA CIBERSEGURIDAD"

Barbastro (Huesca), 22 de julio de 2013

Constituye para mí una satisfacción personal inaugurar hoy estas Jornadas Universitarias de los Pirineos que bajo el título "REALITY CHECK: Descubrir la Identidad Humana en un Mundo Digital", han sido organizadas por la Universidad de Navarra en colaboración con los Colegios Mayores Belagua, Ayete y Mendaur.

Y es un grato placer para mí pronunciar la Conferencia Inaugural de estas Jornadas que gracias al impulso de la Universidad de Navarra, se han convertido ya una referencia entre las escuelas de verano que se desarrollan a lo largo y ancho de España durante estos meses estivales.

La Universidad de Navarra, como institución académica de referencia que es, ha logrado que estas Jornadas conjuguen los espacios de reflexión y el análisis, con el ocio y también con la difusión de los valores fundacionales de la institución.

Por ello a lo largo de esta semana, el atractivo programa que la organización ha preparado, aborda la incontestable influencia que las nuevas tecnologías tienen en diferentes aspectos de las personas en unos difíciles tiempos actuales, de crisis económica, crisis social y de valores.

Amigas y amigos

La llegada de Internet a nuestras vidas y la generalización de su uso ha supuesto no solo un profundo cambio tecnológico, sino sobre todo, un profundo cambio en nuestras vidas.

Las formas de trabajo, las relaciones económicas y laborales, la interlocución con la Administración, el comercio, y hasta la manera de relacionarse entre las personas han sufrido una profunda transformación que no tiene vuelta atrás.

La revolución habida por la llegada a nuestras vidas de internet tiene una dimensión histórica, me atrevería a decir que, similar a la que supuso la invención de la imprenta por Gutenberg hacia 1440 en la difusión del saber, o al impacto en la medicina, con el descubrimiento de la penicilina por parte de Fleming en 1928.

Les voy a dar unos datos del impacto que tiene Internet en nuestras vidas:

- A finales de 2012, según datos de diversas consultoras ya hay cerca de 2.400 millones de usuarios de internet en el mundo; en Europa hay 519 millones, lo que supone un 63% de penetración.
- Y los usuarios de correo electrónico son más de 2.200 millones de personas.
- Existen en el mundo 638 millones de páginas web.
- Por otra parte, el tiempo global que pasamos todos los usuarios de internet en línea por mes es de 35.000 millones de horas.
- Las redes sociales, que son esta nueva manera de relacionarse entre las personas, especialmente entre los más jóvenes (con más de 800 millones de actualizaciones en Facebook y 250 millones de tweets en Twitter al día), son la actividad a la que más tiempo dedican los usuarios de internet (un 22%), seguidas de las búsquedas (hay más de 1.000 millones de búsquedas al día en Google), lectura de contenidos, correos electrónicos, etc.
- En lo que respecta a España, en el EGM de marzo de 2013 sobre Internet, se destacaba que casi 25 millones de españoles han sido usuarios de internet en el último mes, lo que supone un índice de penetración del 63%.
- En el 67% de los hogares españoles ya se dispone de banda ancha fija.
- Y debo señalar que el comercio electrónico ha crecido muy significativamente en el último año en España, pues los ingresos generados en este comercio ya alcanzaron a finales de 2012, más de 2.500 millones de euros, un 20% aprox. más que en el año anterior.
- Destaquemos, además, que según el informe anual de Telefónica, España es el país de Europa en el que más penetración han tenido los teléfonos llamados smartphones, con un 63% entre los usuarios de telefonía móvil.
- Ello hace que 6 millones de españoles ya sean, mejor dicho ya seamos, “comunicadores digitales permanentes”, viviendo las 24 horas del día conectados a la red.

Por último, y como Ministro del Interior me llena de orgullo que el twitter del Cuerpo Nacional de Policía ya tenga 545.473 seguidores, a poca distancia del FBI.

Sin duda puede afirmarse que Internet ha sido una revolución que ha cambiado nuestras vidas ofreciéndonos oportunidades que hasta ahora no teníamos, facilitándonos la vida, pero también haciéndonos más vulnerables.

Alumnas y alumnos
Quiero hablarles de los riesgos y amenazas que presenta la red desde mi perspectiva de Ministro del Interior de España; voy a hablarles de la Ciberseguridad, entendida ésta como el tratamiento global integrado ante las amenazas presentes en lo que denominamos el ciberespacio.

El ciberespacio es en primer lugar la red de infraestructuras físicas compuestas por equipos y redes: son tanto los ordenadores, los sistemas de almacenaje de memoria, los dispositivos móviles, como las redes telefónicas, de fibras ópticas, las intranets e internet, el espacio radioeléctrico y las redes wifi.

Junto a la infraestructura física, en segundo lugar, es también la realidad llamémosla inmaterial de programas informáticos, software, así como la incuantificable cantidad de información digital almacenada en todo tipo de soportes.

Por último también es ciberespacio el ámbito de lo privado del usuario, sean empresas, instituciones públicas/ privadas, o los hombres y mujeres que usan estas tecnologías y estas redes.

El delincuente cibernético se presenta como un enemigo invisible que realiza un negocio criminal de bajo riesgo y alta rentabilidad, y que lo puede llevar a cabo desde cualquier del mundo. Les pongo un ejemplo muy gráfico: un ciberdelincuente en Nueva Zelanda puede estar comprando en un comercio on line de Alemania utilizando los datos de una tarjeta de crédito sustraídos por un hacker español en una base de datos en Japón.

El alojamiento de los servidores y las empresas de Internet en diferentes lugares del mundo con distintas legislaciones y en muchos casos con regímenes políticos dispares, y un modelo de negocio y unas organizaciones

criminales muy distintas a la delincuencia organizada tradicional hacen que la lucha contra el cibercrimen sea muy complicada.
A ello hay que unir el hecho de que Internet permite un modelo en el que no hay jerarquía y sí diferentes grupos comercializando información financiera, malware, troyanos, orientados a cometer delitos.
Y es que después de la prostitución y el tráfico de drogas, el delito más lucrativo a nivel mundial es el cibercrimen. Para darnos cuenta de las magnitudes de las que hablamos les aporto dos datos:

- La Administración de Estados Unidos afirma que en el mundo se sufrieron pérdidas debidas al cibercrimen en 2012 equivalentes a 1 billón de dólares, aproximadamente, el PIB de España en ese año;
- Los ataques cibernéticos aumentaron un 30 por ciento entre 2011 y 2012 y, en el último año, afectaron a unas 550 millones de personas en todo el mundo.

De esta manera, ¿cuáles son las principales amenazas y riesgos? Puedo enumerarles algunas de las principales amenazas y riesgos que encontramos en el ciberespacio:

1º) La Delincuencia Organizada:
Como antes les decía, el ciberespacio es un ámbito en el que los delincuentes pueden llevar a cabo delitos con un bajo riesgo pero que les produce enormes beneficios económicos.

Puede ser creando Malware, infectando y dañando los ordenadores, puede ser robando los datos bancarios, financieros y personales, o usando de manera fraudulenta los números de las tarjetas de crédito.

En este campo, el Ministerio del Interior ha estado muy activo en la lucha contra este tipo de delincuencia: así por ejemplo, quiero destacar la llamada operación “Ramson”, llevada a cabo por el Cuerpo Nacional de Policía en la que se detuvo en Málaga a 10 personas originarias de países del Este. Este Malware infectó a millones de ordenadores en todo el mundo, bloqueando los equipos y solicitando para su desbloqueo el pago de 100€.

2º) El Ciberterrorismo
El ciberespacio también se ha convertido en el nuevo campo donde los grupos terroristas pretenden llevar a cabo sus ataques contra los Estados, contra sus administraciones, sus empresas, o sus ciudadanos.

Desde cualquier lugar del mundo, con un riesgo mínimo para el agresor y a través de las redes digitales se pueden llevar agresiones sobre objetivos estratégicos o infraestructuras críticas de un país, que produzcan terribles daños en el mismo.

Además, la red está sirviendo como vemos claramente en el terrorismo internacional de signo yihadista, de lugar de adoctrinamiento, de propaganda, de reclutamiento y de hasta adiestramiento.

Es el caso del fenómeno que se ha venido a llamar de los "lobos solitarios". Como tristemente se ha comprobado en Boston, Londres o París recientemente, unos sujetos que habían sido adoctrinados en el ciberespacio, han cometido terribles actos de terrorismo que no solo causan dolor, sino que van contra nuestra normal convivencia en paz y libertad.

Como línea de trabajo de este Ministerio del Interior en la lucha contra el ciberterrorismo yihadista, quiero aprovechar para recordarles que en el Consejo de Ministros de Interior-JAI desarrollado el día 7 de junio en Luxemburgo, insté a la modificación de la Decisión Marco de 2008 con la inclusión en la definición de terrorismo del concepto de adiestramiento pasivo, con el fin de prevenir la actuación de los "lobos solitarios".

Se trata de atacar de raíz el problema interviniendo en el momento en que estas personas son adiestradas, entre otros lugares, en las webs dedicadas a ello, trabajando junto a nuestros socios europeos, en perfecta cooperación.

3º) El Espionaje industrial

Es una amenaza real y de enorme trascendencia económica y estratégica. En un mundo tan competitivo y globalizado, en el que el conocimiento es el principal activo de las empresas, su know-how, su I+D o sus bases de datos, son elementos susceptibles de ser sustraídos y vendidos a empresas competidoras en cualquier lugar del mundo.

4º) El llamado "Hacktivismo"

Los ataques que conocemos como "Denegaciones de Servicio" son una seria amenaza para el buen funcionamiento del ciberespacio. A veces se presentan como reivindicaciones políticas, lo cual no oculta su motivación económica, ya que su objetivo es robar datos, perjudicar los servicios de una empresa de la competencia, o simplemente dañar como en el caso de los ataques a webs institucionales.

Precisamente el 28 de abril de este año el Cuerpo Nacional de Policía, en colaboración con el FBI y la policía holandesa, detuvo en Granollers al responsable del mayor ataque cibernético de denegación de servicio de la historia, que logró colapsar internet.

5º) Amenazas para los Menores

Ante los niños y adolescentes, que son usuarios habituales de una Red que forma parte natural de sus vidas, se presentan graves amenazas potenciales que les pueden perjudicar tanto en su normal educación y adquisición de valores, como en su propia integridad y privacidad.

La costumbre de compartir cada vez más datos privados en las redes sociales como sus fotos (el 91% cuelga fotos propias), el nombre de su colegio (el 71%) o su teléfono (el 20%), puede acabar convirtiéndose en un peligro si se da un uso irresponsable de las redes sociales.

De esta manera el menor puede caer víctima de redes de pornografía, ser víctimas de acoso sexual (=grooming), o de vejaciones (=ciberbulling).

Señoras y señores

Como ustedes son conscientes, la ciberseguridad se ha convertido, por tanto, en un aspecto preeminente en todos los países debido a la dependencia tecnológica que todos tenemos.

Así, por ejemplo, nuestras actividades económicas y comerciales, el abastecimiento energético, las telecomunicaciones, un sistema financiero en red, las relaciones sociales, o el funcionamiento diario de los gobiernos dependen de una red correcta y segura.

Esta dependencia tecnológica exige a los gobiernos potenciar la prevención, detección y respuesta en materia de ciberseguridad. Sin embargo, el reto de la ciberseguridad no es solo de la Administración Pública. Para afrontar este reto debemos establecer mecanismos que garanticen una adecuada cooperación lo público y lo privado, y a todos los niveles, tanto nacional como internacional, especialmente en nuestro ámbito europeo.

Tenemos que poner el énfasis en la coordinación de esfuerzos, en la mejora de nuestra seguridad, y en el intercambio de información entre todos los agentes y organismos implicados, cuestión fundamental para reducir el número de delitos tecnológicos.

De esta manera pese a las amenazas, el ciberespacio será lo que debe ser: un espacio de libertad, un lugar para las oportunidades, y en definitiva, un lugar donde los ciudadanos, empresas e instituciones puedan desarrollar sus actividades, sean éstas de ocio o de negocio, sin nada que temer.

El objetivo de la seguridad en el ciberespacio es triple:

1º- Mantener el dinamismo de un medio nuevo que posee un enorme potencial de transformación económica y social, mediante procedimientos legislativos y normativos ágiles y flexibles, pues este es un sector en constante cambio y evolución. Nuestras economías tienen una dependencia activa respecto del ciberespacio. Las nuevas tecnologías de la información posibilitan nuevas actividades económicas impensables hace tan sólo una década, transformando antiguas actividades empresariales, facilitando soluciones tecnológicas, rebajando costes y acercando mercados.

2º- Proteger la privacidad de los usuarios: La Estrategia de ciberseguridad de la Unión Europea, aprobada el 7 de febrero de este año, llama a proteger en el ciberespacio los derechos fundamentales, la libertad de expresión y, como no, los datos personales y la intimidad. Por ello todo intercambio de información a efectos de ciberseguridad en que se manejen datos personales debe cumplir la normativa de protección de datos de la UE y tomar plenamente en consideración los derechos de las personas en este ámbito.

3º- Asegurar el ciberespacio, mejorando las capacidades de prevención, detección y respuesta; protegiendo a las administraciones públicas e infraestructuras críticas; luchando contra la ciberdelincuencia y el ciberterrorismo; reforzando la cooperación internacional; mejorando las capacidades del sector privado y la base de conocimientos y competencias; y creando una cultura de ciberseguridad.

Tras esta exposición sobre las ventajas y los riesgos de Internet, quiero hablarles de lo que está haciendo el Gobierno de España con respecto a la Ciberseguridad, a la que hemos considerado como uno de los principales ejes estratégicos de acción para los próximos años, ya que es el cibercrimen, junto al terrorismo internacional, algunas de las mayores amenazas que tiene nuestro sistema de libertades; por ello así ha sido contemplado en la Estrategia de Seguridad Nacional aprobada el pasado 31 de mayo.

En el ámbito del Ministerio del Interior que tengo el honor de dirigir, ya se ha avanzado considerablemente durante estos años en la mejora de nuestras capacidades, con el fin de ofrecer una adecuada protección cibernética.

El objetivo más importante en el que estamos trabajando en la actualidad, es en la elaboración de una Estrategia Española de Ciberseguridad, que creemos podrá ser presentada antes de 2014.

Para ello estamos colaborando todos los Ministerios competentes en la materia, desde la posición de liderazgo de mi Departamento, que tiene el mayor conocimiento técnico y operativo, además de unidades y organismos con un éxito acreditado en la lucha contra la ciberdelincuencia y el ciberterrorismo.

Esta Ciberestrategia posibilitará que, por un lado, los diferentes departamentos del Gobierno puedan coordinar sus actividades entre sí, y que por otro puedan, a su vez, establecer una adecuada coordinación con las empresas privadas proveedoras de servicios esenciales y con las instituciones relevantes en el ámbito internacional.

No obstante, también se ha venido trabajando intensamente en una tercera vía, complementaria de las dos anteriormente citadas, y que se refiere a la mejora de la protección del propio Sistema Tecnológico frente a amenazas que tienen como objetivo último dañar y atacarlo directamente. Es lo que hemos denominado la “protección de las infraestructuras críticas”.

Con este objeto, en España se creó en 2007 el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), organismo coordinador de todas las medidas que se llevan a cabo a nivel nacional y punto de contacto a nivel internacional.

Para dar respuesta a estas tres líneas de trabajo, el Ministerio del Interior, tanto la Guardia Civil como el Cuerpo Nacional de Policía, dispone de unidades altamente especializadas para la investigación de cualquier acción ilícita en el ámbito del ciberespacio, y con capacidad de adaptarse de forma continua a un entorno tremendamente exigente y en constante cambio.

A lo largo del tiempo que llevamos de legislatura, en diferentes foros, he transmitido mi compromiso personal con la ciberseguridad, anunciando y más tarde poniendo en marcha medidas contundentes y eficaces en este

sentido, a pesar de que vivimos en una época de presupuestos más restrictivos y de reducción de gastos, pues hablamos de una materia capital para nuestro país.

En este sentido, y con el objetivo fundamental de reforzar las capacidades, tanto de las Fuerzas y Cuerpos de Seguridad del Estado como del CNPIC, los Ministerios del Interior y de Industria, Energía y Turismo del Gobierno de España, firmaron en octubre de 2012 un Convenio marco de colaboración en materia de ciberseguridad.

El desarrollo del mencionado convenio, que están llevando a cabo grupos de expertos de ambos ámbitos, combina dos ideas fundamentales que son, que el ciberespacio debe ser un entorno donde se posibilite el desarrollo competitivo en este mundo globalizado de la actividad industrial, empresarial y privada, pieza básica en el crecimiento económico que España necesita; y que estas posibilidades deben desarrollarse en un marco con la seguridad garantizada, minimizando los posibles riesgos.

La fusión de las capacidades y de la excelencia tecnológica del Ministerio de Industria, Turismo y Comercio, con la experiencia, conocimientos y formación del personal de las Fuerzas y Cuerpos de Seguridad del Estado, dará lugar a una nueva serie de proyectos tecnológicos y una gran mejora en materia de ciberseguridad en España.

Por otra parte, permítanme también citarles otras iniciativas llevadas a cabo hasta el momento. Por ejemplo, está pendiente en este momento la inauguración oficial en la ciudad de León del primer equipo de respuesta a ciberincidentes en infraestructuras críticas y estratégicas, el denominado CERT para las infraestructuras críticas. Este CERT IC que se viene a sumar a los CERT ya existentes (CERT-FAS del Ministerio de Defensa, Centro Criptológico Nacional del CNI, CNPIC de la Secretaría de Estado de Seguridad de Interior, y CERT INTECO del Ministerio de Industria, Energía y Turismo), y que es fruto del trabajo entre los Departamentos de Industria e Interior, tiene como misión fundamental asistir a las empresas y organizaciones que operan nuestras infraestructuras en su labor de prevención, detección, evaluación y respuesta ante posibles incidentes.

Por lo que respecta a los recursos humanos y técnicos del Ministerio, estamos reorganizando y reforzando las unidades operativas de las Fuerzas y Cuerpos de Seguridad del Estado en lo referente a la persecución de delitos cibernéticos, duplicando dichas unidades, y multiplicando así las

capacidades existentes hace poco tiempo, tarea en la que se seguirá haciendo esfuerzos en los próximos meses.

Por otra parte, en el seno del CNPIC, hemos anunciado la creación de una Oficina de Coordinación Cibernética que garantizará la confidencialidad de los datos que sean susceptibles de tratamiento e investigación por parte de las Fuerzas y Cuerpos de Seguridad del Estado.

Señoras y señores,
Termino ya deseándoles los mayores éxitos en estas Jornadas Universitarias que hoy se inician.

Es una semana apasionante la que tienen por delante, con temas interesantes y debates en los que el intercambio de ideas favorecerán una visión más amplia de esta revolución silenciosa que ha llegado y a todos nos afecta.

Como Ministro del Interior del Gobierno de España quiero resaltarles, que siendo la Red un mundo de oportunidades que debemos aprovechar para un mejor desarrollo como personas, el Gobierno de España seguirá velando por los derechos, las libertades y la seguridad de los ciudadanos, también en el ciberespacio.