Tribuna Norteamericana
nº30, septiembre 2019

La historia de... Talgo en EE.UU.
por Nora Friend

I-ntentando e-xplicar lo que significa la ciberseguridad
por Ángel Gómez de Ágreda

Los claroscuros de la ciberseguridad
por Yaiza Rubio

Ciberdelincuencia en España, un desafío para el Cuerpo Nacional de Policía
por Pedro Pacheco

Universidad de Alcalá
Instituto Universitario de Investigación en Estudios Norteamericanos
"Benjamin Franklin" de la Universidad de Alcalá

El Instituto Franklin-UAH (fundado originalmente como "Centro de Estudios Norteamericanos" en 1987) es un organismo propio de la Universidad de Alcalá que obtuvo el estatus de "Instituto Universitario de Investigación" en el 2001 (Decreto 15/2001 de 1 de febrero; BOCM 8 de febrero del 2001, no 33, p. 10). Su naturaleza, composición y competencias se ajustan a lo dispuesto en los Estatutos de la Universidad de Alcalá de acuerdo al Capítulo IX: "De los Institutos Universitarios" (artículos del 89 al 103). El Instituto Franklin-UAH tiene como misión fundamental servir de plataforma comunicativa, cooperativa y de unión entre España y Norteamérica, con el objetivo de promover el conocimiento mutuo. El Instituto Franklin-UAH desarrolla su misión favoreciendo y potenciando la creación de grupos de investigadores en colaboración con distintas universidades norteamericanas; impartiendo docencia oficial de postgrado (másteres y doctorado en estudios norteamericanos); difundiendo el conocimiento sobre Norteamérica mediante distintas líneas editoriales; y organizando encuentros académicos, de temática inherente a la propia naturaleza del Instituto, tanto de carácter nacional como internacional.

ISSN: 1889-6871
Depósito Legal: DL M-26597-2016
Impreso en España - Printed in Spain
Impresión: Cimapress

Tribuna Norteamericana es una publicación del
Instituto Franklin-UAH

Universidad de Alcalá
c/ Trinidad, 1
28801 Alcalá de Henares, Madrid. España

Tel: 91 885 52 52

www.institutofranklin.net

Tribuna Norteamericana *se distribuye gratuitamente entre sus suscriptores.*
Si desea recibir esta publicación, contacte con: publicaciones@institutofranklin.net

EL DIRECTOR OPINA

Francisco Manuel Sáez de Adana

Catedrático de la Universidad de Alcalá

Director

Estimado lector:

Es un placer y una enorme responsabilidad tomar el relevo de José Antonio Gurpegui al frente de la revista *Tribuna Norteamericana*. Han sido diez años en los que el buen hacer de José Antonio y del equipo del Instituto Franklin han convertido esta revista en una referencia en lo que se refiere a la política, la economía, la sociedad y la cultura de Estados Unidos. Por suerte, el equipo de la revista se mantiene, por lo que esa responsabilidad es más fácil de afrontar, pero en todo caso espero estar a la altura del trabajo realizado hasta la fecha. En todo caso, querido José Antonio, quiero agradecer tu confianza y espero que en esta nueva etapa la revista siga despertando el interés del lector de la misma forma que la etapa anterior.

Para ello este número trata un tema de vital importancia en nuestros días, no solo en los Estados Unidos, sino a nivel global. Y es que en los últimos años se ha incrementado enormemente la preocupación por la seguridad informática o, como se conoce más comúnmente, la ciberseguridad. No es, desde luego, una preocupación que aparezca de repente, pero lo cierto es que el incremento de las llamadas *fake news*, la alarma que ha creado el hecho de que el intercambio de información que todos realizamos en nuestra actividad cotidiana a través de las redes pueda ser espiado por diferentes personas y organismos y el hecho de que, tanto nuestra vida tanto profesional como la personal cada vez dependan más de los equipos informáticos y de la comunicación entre estos a través de la redes, hace que la preocupación por todo lo concerniente con la seguridad en las tecnologías de la información sea un tema de gran actualidad.

Sin embargo, no siempre se tiene un conocimiento exacto por parte del ciudadano sobre todo lo relacionado con la ciberseguridad. Por esto en este número de TN contamos con tres especialistas de reconocido prestigio con el objetivo de mostrarnos algunos aspectos clave de este tema tan complejo. Para empezar, el coronel Ángel Gómez de Agreda nos explica el significado de lo que conocemos por ciberseguridad, poniendo énfasis en su importancia en la sociedad de nuestros días y en un concepto asociado a la seguridad informática de tanta importancia como es la ciberguerra. Yaiza Rubio, analista de seguridad en ElevenPaths, nos muestra a través de su artículo que la situación actual no es tan dramática como en muchas ocasiones se percibe desde fuera gracias a la enorme labor que se está haciendo en los últimos años en el ámbito de la investigación en ciberseguridad. Finalmente, el comisario Pedro Pacheco, Jefe la Unidad Central de Ciberdelincuencia del Cuerpo Nacional de Policía, nos cuenta la labor que, desde este cuerpo se está realizando en materia de cibeseguridad y los enormes desafíos que esta tarea supone. Además, completa el número, dentro de la sección "La historia de", la experiencia de Talgo en los Estados Unidos, a través de su Vicepresidenta de Negocio y Relaciones Institucionales, Nora Friend.

Un número, por tanto, desde mi punto de vista, de gran interés. Punto de vista que, espero, el lector comparta.

Francisco Manuel Sáez de Adana

Nora Friend

Licenciada en Management and Organizational Behavior por la facultad School of Management de la Universidad de Boston, Massachusetts.

Es vicepresidenta de Desarrollo de Negocio y Relaciones Institucionales en Talgo Inc., filial de Talgo en los Estados Unidos con sede central en Seattle, Washington y oficinas en los estados de la Florida; Washington D.C.; y Wisconsin. Se incorporó a Talgo en 1994 y a lo largo de los años ha desarrollado su carrera profesional asumiendo responsabilidades hasta liderar marketing, relaciones gubernamentales, relaciones institucionales y de comunicación. Además, lidera el desarrollo de negocio y expansión en Norteamérica. Actualmente es miembro del Comité Ejecutivo del US-Spain Council, y participa en comités de las asociaciones sectoriales como American Public Transportation Authority y es miembro del Transportation Research Board, Midwest High Speed Rail Association, United States High Speed Rail Association, Womens Transportation Seminar, Rail Progress Institute y Rail Passenger Association, entre otras.

Vicepresidenta de Desarrollo de Negocio y Relaciones Institucionales en Talgo Inc.

Twitter: @TalgoGroup

La historia de...
TALGO EN EE. UU.

Nora Friend

1 *Orígenes*

Talgo es una empresa tecnológica española especializada en el diseño y fabricación de trenes y equipos de mantenimiento, así como en la prestación de servicios de mantenimiento a operadores ferroviarios de todo el mundo. Es el principal suministrador de trenes de alta velocidad en España.

Talgo nació en el año 1942 con un concepto innovador de tren ligero y articulado que permitió mejorar sustancialmente parámetros clave en la operación de los trenes de la época: se redujo el consumo energético, el esfuerzo tractor y los tiempos de viaje (sin necesidad de inversión en infraestructura), se incrementó el confort de los pasajeros y se recortaron los gastos de explotación de los operadores ferroviarios.

Esta revolución supuso un antes y un después en el sector, no solo en España sino a nivel internacional, y posicionó a Talgo en la vanguardia de la industria ferroviaria. Desde entonces y hasta nuestros días, Talgo ha mantenido este carácter innovador con la mejora permanente de sus productos y la creación de nuevas soluciones adaptadas a las necesidades de transporte de sus clientes (operadores ferroviarios de todo el mundo) y, con ello, de toda la sociedad. Las 71 patentes que actualmente posee la compañía han contribuido además al desarrollo económico e intelectual de España.

Tras más de 75 años de historia, la compañía se ha convertido en un fabricante global de trenes de pasajeros, con un alto grado de especialización en el diseño, fabricación y mantenimiento de trenes de alta velocidad. En la actualidad es líder en este segmento, como primer suministrador de trenes de alta velocidad en España, y se ha convertido en una de los principales suministradores de vehículos ferroviarios a nivel mundial.

En España circulan hoy 46 trenes Talgo de muy alta velocidad (>300km/h) y 45 trenes Talgo de alta velocidad (>250km/h). Estos últimos incorporan un innovador sistema cambio de ancho de vía y que permiten aprovechar al máximo las nuevas infraestructuras ya construidas, pero aún no completadas. Adicionalmente,

Hoy en día el servicio Amtrak Cascades© opera más de 4000 servicios anuales con los Talgo Serie 6 y 8

El corredor tiene una longitud de 467 millas, 300 millas en el estado de Washington, 134 millas en Oregón y 33 millas en British Columbia (Canadá)

unos 1000 coches Talgo forman composiciones remolcadas que circulan a velocidades de hasta 220 km/h, tanto en líneas que discurren por vías de un solo ancho de vía como en aquellas que utilizan dos anchos y, por lo tanto, necesitan que los trenes vayan equipados con un sistema especial de cambio automático. En los últimos 35 años Talgo ha fabricado un total de más de 260 cabezas tractoras y más de 4000 coches para clientes de todo el mundo.

Los trenes Talgo han circulado o circulan así por países como España, Portugal, Francia, Suiza, Alemania, Italia, Estados Unidos, Kazajistán, Uzbekistán, Rusia, Arabia Saudí, Bosnia Herzegovina y Canadá.

2 La llegada a los EE. UU.

Talgo, Inc. tiene una larga y exitosa historia en Estados Unidos. En 1944 Talgo se asoció con American Car and Foundry para fabricar en América los primeros Talgo que se utilizarían en operación comercial, tanto en España como en la Costa este de Estados Unidos. De hecho, los trenes Talgo fueron operados hasta principios de los años 60 en el continente americano, y solo fueron retirados del servicio cuando los Estados Unidos decidieron apostar por el automóvil y avión como medio de trasporte, a expensas del ferrocarril.

La historia en los Estados Unidos continúa en 1988, cuando el operador Amtrak realizó ensayos con los Talgo equipados con un innovador sistema de pendulación natural que permitía circular con más rapidez y confort en las vías existentes. Los ensayos demostraron que utilizando trenes Talgo se podía reducir sustancialmente el tiempo de viaje entre las ciudades de Boston y Nueva York, cuyas vías transcurren a través de un trazado sinuoso.

En 1994 Talgo volvió a entrar al mercado americano en asociación con RENFE al firmar un contrato de arrendamiento de un tren Talgo Pendular con el Departamento de Transporte del estado de Washington (WSDOT) quien a su vez puso este tren en servicio comercial en el Corredor Pacific Northwest con recorrido desde Seattle hasta Portland. Tan grande fue el éxito de este servicio que WSDOT y el operador nacional ferroviario (Amtrak) decidieron comprar un total de cuatro trenes y extender el contrato original de seis meses durante dos años, mientras se fabricaban un total de cinco trenes. Talgo vendió un quinto tren a WSDOT en noviembre de 2003 para satisfacer la creciente demanda del corredor. Como resultado de este contrato, Talgo decidió instalarse en el estado de Washington para proveer el mantenimiento integral del material vendido.

3 Talgo Serie 6 y 8

Los trenes de la Serie 8 son el último desarrollo de Talgo para el mercado norteamericano, y han sido específicamente diseñados para ofrecer el mejor servicio en este mercado, diseñados para alcanzar una velocidad máxima de 125 mph. Cumplen por ello con todos los estándares fijados por la agencia federal reguladora FRA (Federal Railroad Administration), una de las más exigentes del mundo en materia de accesibilidad universal y resistencia estructural en caso de colisiones. El éxito operativo de las cinco composiciones Talgo fabricadas a finales de los años 90 para el servicio Amtrak Cascades© entre Portland y Vancouver fue determinante para que en 2009 se ejecutase un nuevo pedido de material rodante. El Departamento de Transporte de Oregón (ODOT) realizó la compra de dos trenes Talgo Serie 8 en febrero de 2010 aumentando así la flota de trenes ya existentes en el corredor de Amtrak Cascades a un total de 7 trenes que se unieron a los 5 ya existentes. Los trenes para el Departamento de Transporte de Oregón fueron entregados a finales del 2013 y puestos en servicio comercial en enero de 2014.

Talgo Serie 8

El estado de Wisconsin recibió 823 millones de dólares de los fondos ARRA (American Recovery and Reinvestment Act Funds) destinados por el Gobierno del ex presidente Obama para la construcción de la línea de alta velocidad

Hoy en día el servicio Amtrak Cascades© opera más de 4000 servicios anuales con los Talgo Serie 6 y 8. El corredor tiene una longitud de 467 millas, 300 millas en el estado de Washington, 134 millas en Oregón y 33 millas en British Columbia (Canadá). Más de 744 000 pasajeros utilizaron el servicio en 2015, en el 2017 el récord de pasajeros fue de 811 000.

Por otra parte, con la vista puesta en incrementar la oferta tanto en la costa occidental como en la ruta Wisconsin y Chicago, en el 2009 el gobernador Doyle anunció la compra de dos trenes Talgo Serie 8 para ser utilizados en el corredor Hiawatha (Milwaukee a Chicago). El gobernador Doyle celebró la apertura de la nueva planta de montaje y fabricación de Talgo en Milwaukee, Wisconsin. El estado de Wisconsin recibió 823 millones de dólares de los fondos ARRA (American Recovery and Reinvestment Act Funds) destinados por el Gobierno del ex presidente Obama para la construcción de la línea de alta velocidad. De estos fondos, 12 millones de dólares serían para mejorar el servicio de la línea entre Chicago y Milwaukee. El gobernador sucesor rechazó

Talgo Inc. tiene su oficina central en Seattle (Washington) y también tiene una oficina en la capital federal, Washington D. C. con el objetivo de desarrollar el mercado y tratar asuntos gubernamentales. Asimismo, cuenta con oficina en Florida y fábrica en Milwaukee

el proyecto y en consecuencia la compra de los dos Talgo Serie 8 destinados a este servicio. Dichos trenes están listos y disponibles para eventualmente incorporarse en la red ferroviaria del mercado estadounidense.

Todos los coches que conforman la nueva Serie 8 han sido fabricados en la planta instalada por Talgo en la ciudad de Milwaukee. Su mantenimiento se realiza desde las instalaciones de Seattle, con las máximas garantías y con el objetivo de ofrecer la máxima disponibilidad. Los coches son completamente accesibles, y ofrecen al viajero todas las facilidades para aprovechar el viaje, ya sea trabajando o descansando. Cuentan por eso con conectividad gratuita y sistemas de entretenimiento.

Los viajeros que utilizan los trenes Talgo en el servicio Amtrak Cascades© no solo cruzan la frontera entre Estados Unidos y Canadá sin moverse de su asiento sino que además esscapan durante un tiempo del frenesí de las metrópolis. El diseño interior de los coches y el servicio a bordo han sido pensados para ofrecer una experiencia de viaje sin parangón en todo Estados Unidos.

Los trenes Talgo en el mercado norteamericano han supuesto un gran éxito por sus características tecnológicas que lo diferencian de la competencia. Su construcción ligera y su capacidad de pendulación natural lo convierten en un producto más eficiente y económico para el mercado y recursos limitados del transporte ferroviario de Estados Unidos. Otra parte del éxito en el corredor occidental es el resultado de una buena relación con los Departamentos de Transporte de Oregón (ODOT) y Washington (WSDOT), la operadora Amtrak y Burlington Northern Santa Fe y Union Pacific (los dueños de la vía).

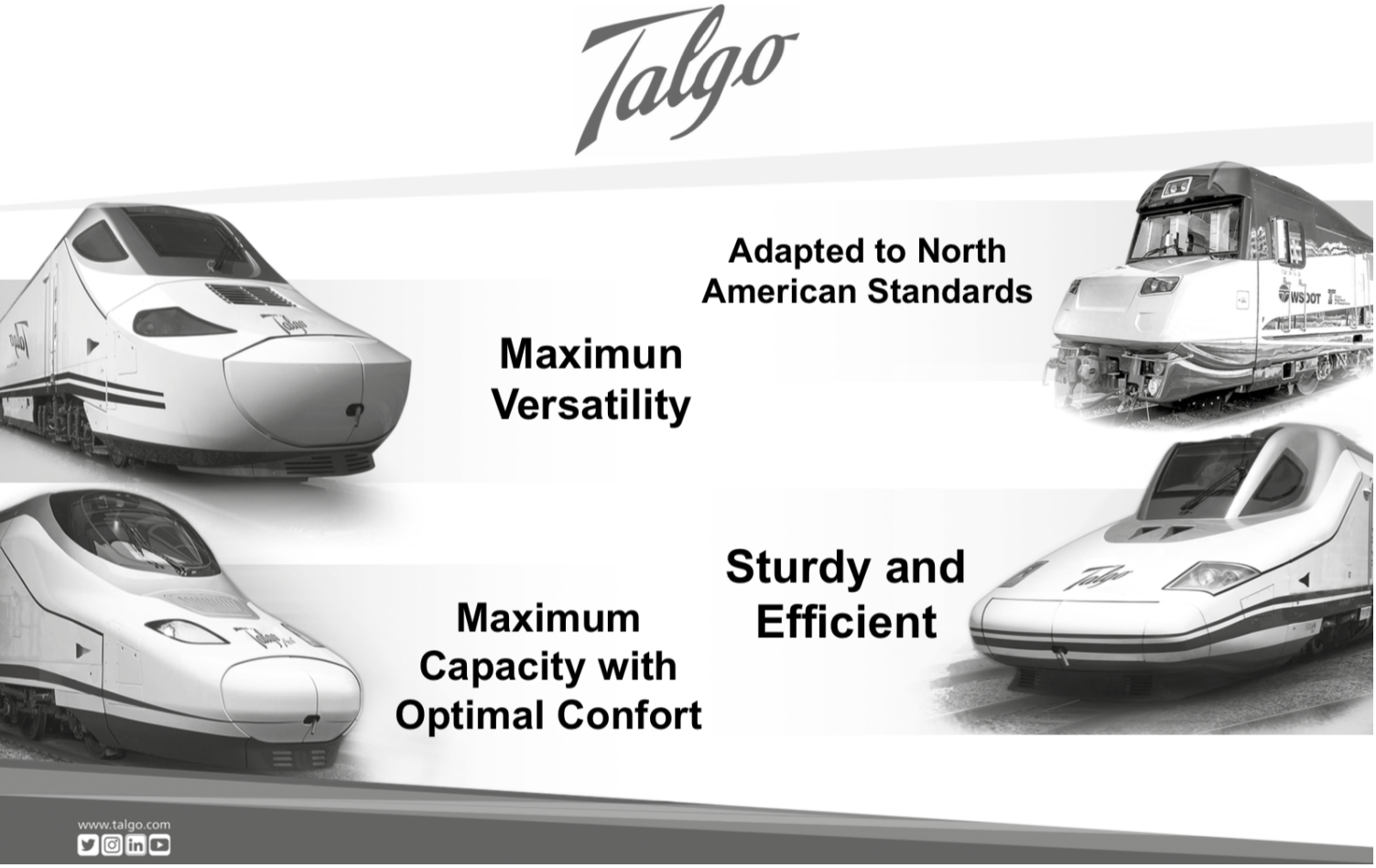
4 Mantenimiento integral como factor diferencial y estratégico

El sistema de mantenimiento Talgo es un elemento clave del éxito de la implantación en este exigente mercado. Está basado en actuaciones preventivas, y tiene su fundamento en la experiencia acumulada durante más de 75 años. Talgo proporciona asistencia técnica y la gestión de las operaciones de mantenimiento de los trenes asumiendo completa responsabilidad de la operación durante el ciclo de vida del producto, e incluye inspecciones diarias, limpieza, intervenciones mayores, rehabilitaciones periódicas y modificaciones para actualizar sistemas obsoletos o requeridos por cambios tecnológicos. A tal fin, Talgo tiene firmados sendos contratos de mantenimiento con Amtrak y con el estado de Washington desde 1999.

5 La rehabilitación de coches como estrategia de diversificación

Talgo continúa abriéndose campo en el mercado estadounidense con la rehabilitación de coches para agencias que operan servicios de cercanías y metro. En septiembre de 2016, la Autoridad del Transporte Metropolitano de Los Ángeles (LACMTA) adjudicó a Talgo el proyecto de renovación de varios sistemas y subsistemas críticos de 74 vehículos asignados a la denominada Línea Roja del metro de la ciudad. El contrato se comenzó con una orden inicial de 38 vehículos, y luego se ejecutó la opción para otros 36 vehículos.

Talgo avanza con entusiasmo con esta oportunidad demostrando cómo su larga experiencia en la renovación de material rodante mejorará el rendimiento de los vehículos que prestan servicio en el metro de Los Ángeles garantizando la seguridad, fiabilidad, disponibilidad y mantenibilidad de esta, y con ello los ingresos comerciales y el buen estado del parque de material rodante. Talgo ha estado trabajando durante un par de años con suministradores que vienen demostrando su experiencia en el aprovisionamiento de sistemas de



El alcalde de Milwaukee, Tom Barrett, ha señalado por su parte que la ciudad ve con mucho agrado cómo Talgo expande sus operaciones en ese estado del Midwest

propulsión, frenado, comunicaciones, señalización y otros componentes requeridos por este metro. El alcance del trabajo está repartido entre Milwaukee (Wisconsin) y Los Ángeles (California).

El alcalde de Milwaukee, Tom Barrett, ha señalado por su parte que la ciudad ve con mucho agrado cómo Talgo expande sus operaciones en ese estado del *Midwest*. Es testigo de la alta calidad de las operaciones de fabricación de coches de viajeros que Talgo ha realizado en Milwaukee.

6 *Una visión a largo plazo*

La continua expansión de Talgo en Estados Unidos depende en gran medida de la dotación de subvenciones del gobierno federal hacia los distintos estados que necesitan inversión de capital para mejorar la infraestructura de tal forma que posibilite la circulación de trenes de alta velocidad. Es necesario que el actual gobierno continúe identificando que la alta velocidad ferroviaria es un elemento importante dentro de un esquema intermodal equilibrado, y, para ello, que se sigan dotando aportaciones presupuestarias que, aunque modestas en relación con países europeos como España, muestren la voluntad política de apostar por el ferrocarril como medio de transporte y de creación de riqueza.

Talgo Inc. tiene su oficina central en Seattle, Washington y también tiene una oficina en la capital federal, Washington D. C. con el objetivo de desarrollar el mercado y tratar asuntos gubernamentales. Asimismo, cuenta con oficina en Florida y fábrica en Milwaukee.

Ángel Gómez de Ágreda

Es coronel del Ejército del Aire, Diplomado de Estado Mayor, de Seguridad de Vuelo y de Logística Militar. Máster en Terrorismo por la Universidad Internacional de La Rioja y doctorando por la Universidad Politécnica de Madrid en Ingeniería Industrial.

Piloto de transporte y paracaidista. Fue miembro y jefe de la Patrulla Acrobática de Paracaidismo del Ejército del Aire (PAPEA) y del Equipo Nacional de Paracaidismo. Ha sido profesor en el Departamento de Estrategia y Relaciones Internacionales del Centro Superior de Estudios de la Defensa Nacional (CESEDEN), Jefe de Cooperación del Mando Conjunto de Ciberdefensa y analista geopolítico en la Secretaría General de Política de Defensa, puesto que ocupa actualmente. Ha participado en cuatro misiones internacionales, dos en la Antigua Yugoslavia, una en Afganistán y una en África.

Es autor del libro *Mundo Orwell. Manual de supervivencia para un mundo hiperconectado*.

Coronel del Ejército del Aire

Twitter: @AngelGdeAgreda

I-ntentando e-xplicar LO QUE SIGNIFICA LA CIBERSEGURIDAD

Ángel Gómez de Ágreda

Hace unos años corría por las redes una versión "actualizada" de la pirámide Maslow, la que se toma como referencia para determinar la jerarquía de las necesidades humanas. En la base de la versión original de 1943 aparecían las necesidades fisiológicas como el escalón inferior, más urgente y necesario para las personas. En la adaptación digital, el acceso a Internet se colocaba por debajo de la exigencia de comida, bebida y cobijo, y de la seguridad. Al fin y al cabo, cualquier internauta puede pasarse horas sin comer o beber, pero muchos sufrirían terriblemente con una abstinencia similar de acceso a las redes.

Incluso si seguimos con la parodia que, medio en broma, medio en serio, apareció en numerosos memes, la tozuda realidad nos demuestra que por debajo de ese escalón de acceso digital tenemos que colocar otro que garantice una cierta seguridad de ese acceso. Vivimos en un mundo físico con necesidades fisiológicas y, cada vez más, en uno lógico en el que tenemos necesidades digitales. Sin embargo, como seres humanos, seguimos teniendo en ambos la urgencia de sentir que jugamos en un entorno en el que existen reglas y límites.

Eso no significa que esas reglas y esos límites sean los mismos en ambos entornos. Adelantemos ya desde el principio que no lo son. Y también que confundir las normas y los ritmos de los dos es un error tan grave como frecuente entre los "inmigrantes digitales", aquellos que todavía aprendimos a escribir con lápiz antes que con un teclado. En un mundo estamos hechos de carne y hueso, en el otro de unos y ceros, de datos que conforman lo que serían nuestras actitudes y nuestras aptitudes, nuestras filias y nuestras fobias, nuestras virtudes y nuestros vicios, y que exponemos a miles de millones de personas y cosas que las observan desde el otro lado de la pantalla o el teclado, incluso cuando no estamos siendo conscientes de revelar ningún dato.

Nuestra vida tiene lugar en ambos mundos simultáneamente. Eso supone que estamos antropológica y psicológicamente situados entre lo físico y lo digital. Por lo tanto, nuestros avatares —los nombres que nos representan en el ciberespacio, en nuestro correo electrónico, nuestras redes sociales, etc.— se relacionan entre ellos virtualmente siguiendo patrones sociológicos y políticos. Dentro de los primeros están las amistades y los amores, las relaciones comerciales y grupales que surgen en Internet, pero también los crímenes y la delincuencia cibernéticas. Y entre los políticos tendremos una capacidad de debatir y negociar, de formar alianzas y construir proyectos sin precedentes hasta el momento. Pero también tendremos la que, pese a que nos cueste admitirlo, es la forma última de hacer política: los conflictos y la guerra.

Nos hemos acostumbrado tanto a dejar nuestra seguridad en manos del Estado o de terceros que nos cuesta asumir que tengamos que contribuir activamente a ella

No conviene dramatizar en exceso ni alimentar expectativas exageradas. Internet no es más que un nuevo entorno en el que desarrollar la actividad humana. Un entorno, si se quiere, que potencia todo aquello que hay de bueno y malo en nosotros, que nos permite llevarlo mucho más lejos, a más gente y más rápido. Un entorno incluso más humano que los naturales, ya que lo hemos diseñado nosotros. Es nuestro comportamiento, tanto individual como colectivo, el que determina lo que ocurre en los dos mundos. Nuestra responsabilidad es que siga siendo así.

1 Ciberseguridad

Escribir sobre los riesgos y amenazas de la ciberseguridad a estas alturas conlleva el riesgo de repetir lugares comunes con que nos bombardean la prensa y las redes sociales todos los días. Todo el mundo tiene la idea difusa de que hay virus en el ambiente digital, de que nos intoxican con fake news y de que Alexa nos espía. Y a casi todos parece darles igual. Total, ¿quién va a querer espiarme a mí? ¿No me viene incluso bien que me manden anuncios de ofertas de viajes cuando estoy a punto de irme de vacaciones?

Otra cosa es que tengamos claras las consecuencias de esa falta de seguridad en el ciberespacio. Cuando el anuncio de las vacaciones nos llega con un precio creciente cuanto más interés ponemos en encontrar viajes, cuando los productos que nos ofrecen dependen del lugar desde el que nos conectemos, de nuestro nivel de vida, nuestros hábitos o nuestras creencias y cuando eso supone que una parte del mundo resulta invisible a nuestros ojos porque nunca llega a nuestro móvil o a nuestro portátil, entonces empezamos a ver dónde está el problema.

Pero, para entonces, normalmente ya hemos caído en la trampa de la comodidad. En el viejo dilema entre seguridad y libertad, en el contrato social de Rousseau, hemos dejado que ambos platos de la balanza acaben abajo. Hemos perdido nuestra libertad para elegir porque nos hemos convertido en seres transparentes para aquellos que tienen nuestros datos y que nos entregan la información que consumimos. Privados de la verdad, no solo por la mentira, sino por la ocultación de una parte de la realidad, hemos dejado de tener la capacidad para elegir. Y hemos perdido nuestra seguridad porque era el paso necesario para convertirnos en transparentes.

Hemos dejado nuestra libertad y nuestra seguridad en el mismo cajón en el que hemos depositado nuestros datos. Hemos renunciado a las dos a cambio de la comodidad del acceso inmediato y, aparentemente, gratuito a servicios que no habíamos sentido necesidad de tener hasta ahora o que, incluso, no existían hasta hace unos meses. Estamos camino de convertirnos en seres teledirigidos por empresas o por instituciones que saben todo de nosotros y, por lo tanto, pueden manipularnos impunemente.

Ejemplos de cómo la comodidad, la curiosidad, la conveniencia o la inmediatez nos hacen relajar nuestras defensas se encuentran fácilmente en el día a día. El "reto de los diez años" en que se nos invitaba a subir una foto actual y otra de hace una década, o la aplicación FaceApp, que nos "envejece" siguiendo patrones —bastante simplistas, por cierto— de inteligencia artificial, son solo dos de los múltiples cebos que nos ofrecen para que contribuyamos con nuestros datos a aplicaciones que, después, obtendrán millones de la agregación de los mismos.

No parece que ejemplos como el de *Cambridge Analytica* hayan hecho mucha mella en la mayor parte de la población. Igual que ataques de *ransomware* como el famoso Wannacry tampoco consiguieron concienciar a las empresas de la necesidad de mantener el software de sus equipos actualizado. Nos hemos acostumbrado tanto a dejar nuestra seguridad en manos del Estado o de terceros que nos cuesta asumir que tengamos que contribuir activamente a ella.

Y, sin embargo, la seguridad no es gratuita, ni nunca completa. Ni siquiera es algo que puedas medir como tal. Es más un sentimiento que una realidad tangible. Y es muy fácil sentirse seguro detrás del cristal de una pantalla mientras miramos a la parte del mundo que algunos quieren enseñarnos desde el conocimiento de nosotros que les da estar viendo cada una de nuestras acciones. La libertad tampoco es gratuita (*Freedom is not*

Free reza la frase que se refleja en la fuente del Memorial a los Veteranos de la Guerra de Corea, en Washington). La libertad se construye sobre la verdad y el conocimiento. El hecho de que el conocimiento nos llegue cada vez más a través de Internet hace que la defensa de este sea un elemento crítico en la de la libertad.

Conocer el ciberespacio se convierte en algo tan vital — si no más— como conocer el barrio en el que vivimos, nuestro ambiente de trabajo, las normas sociales y las convenciones por las que nos guiamos, y las reglas jurídicas que definen nuestro comportamiento en el mundo físico. La diferencia fundamental es que una buena parte de ese mundo se rige por leyes naturales inmutables, mientras que el ciberespacio es una construcción humana que evoluciona a un ritmo exponencial, y cuyas leyes, términos y condiciones de uso pueden ser y son revisados constantemente.

Cabe pensar que hemos diseñado un mundo solo aparentemente amigable, basado en una estructura reticular cuya fortaleza está en las relaciones y no en los individuos, que privilegia por lo tanto a los grupos más numerosos, a las corporaciones y los Estados sobre las personas. Un mundo cuya evolución somos incapaces de seguir. Que se basó en su diseño en criterios de usabilidad sin plantearse nunca la seguridad al estar pensado para una comunidad cerrada que se convirtió en universal. Un ciberespacio que creció básicamente desregulado para seguir favoreciendo ese crecimiento desenfrenado, aposentado sobre la idea de un usuario altruista, colaborativo e ilustrado.

Y es cierto que, durante su etapa "hippie", Internet creció pensando que la Declaración de Independencia del Ciberespacio de John Perry Barlow era posible. Creyendo en un mundo en el que la información iba a fluir libre y universalmente para provecho de todos y de cada uno, en el que el ciudadano podría participar directamente en la toma de decisiones aprovechando las conexiones para revivir la democracia ateniense clásica.

Internet proporciona todo este potencial y bastante más. Jamás se habría podido secuenciar el genoma humano o desarrollar la economía del siglo XXI sin esa capacidad para relacionar datos de miles de millones de cosas y personas. Pero la información no fluye siempre libremente, sino que lo hace dirigida y digerida, la participación ciudadana se ve condicionada por esa falta de acceso a la realidad y, a falta de esta verdad, hemos recurrido a la reputación efímera de las redes como criterio para construir nuestras certezas.

Desde luego, tenemos que construir una red segura. Necesitamos diseñar sistemas robustos que garanticen la confidencialidad, integridad y disponibilidad de nuestros datos. Debemos proveernos de soluciones técnicas que hagan muy difícil el acceso a nuestros sistemas, de soluciones sociales que supongan normas de comportamiento cívico en Internet y de soluciones legales que blinden los huecos que se puedan explotar técnica o socialmente. Pero, para todo ello, primero necesitamos comprender qué supone la llegada del ciberespacio y cómo ha cambiado nuestras vidas y nuestros valores.

En un rápido repaso de las principales características distintivas del ciberespacio, más allá de su naturaleza artificial, podríamos empezar por su alcance universal. Las audiencias a las que nos dirigimos a través de las redes no tienen limitación para lo bueno o para lo malo. Es casi imposible para un usuario normal segmentar su relato en función de la audiencia, igual que es complejo acotar la información que se recibe. Esta tremenda exposición obliga a considerar la transparencia como una necesidad básica. Todo lo que está en la nube es susceptible de ser visto por alguien y, con tanta gente y tantos sistemas inteligentes buscando, lo será. Solo desde la construcción de un relato coherente se pueden defender posturas en el futuro sin tener que adoptar maniobras defensivas poco creíbles.

No se trata solo de aquellos datos que transmitimos conscientemente. Como afirma Marta Peirano, el sistema conoce todo sobre cada uno de nosotros. Nuestra forma de teclear, de mover el ratón, de andar cuando llevamos el móvil encima (que es siempre), los horarios a los que realizamos cualquier actividad, los lugares por los que nos movemos, todo forma parte de una gran base de datos que el Gran Hermano va construyendo y de la que va extrayendo un perfil sobre nosotros, como individuos y como grupo, mucho más preciso del que tenemos nosotros mismos.

El gran salto vino de la mano de la movilidad. La cantidad de datos que percibe, acumula y transmite cualquier *smartphone* supone un filón de conocimiento para las compañías que están detrás de su fabricación o funcionamiento. Y, muchas veces, de los Estados que tienen jurisdicción sobre las infraestructuras de dichas empresas. No hay movimiento, por leve que sea, que escape a la sensibilidad de los giróscopos de nuestros móviles. Su función principal no es que hablemos por teléfono —de hecho, cada vez los utilizamos menos para eso— como demuestra el hecho de que se reserven siempre una carga remanente de batería después de dejar de servirnos a nosotros para seguir estando en condiciones de enviar los datos que realmente les dan sentido.

En esas condiciones, ¿no debemos replantearnos el valor de la privacidad en nuestras vidas? No es lo mismo el conocimiento parcial que algunas agencias o empresas tenían sobre nosotros hace unos años que el conocimiento exhaustivo que tienen ahora aquellos que puedan acceder a nuestros datos (y, como ha quedado demostrado, estos están a la venta). Es la misma diferencia que vivir en una gran ciudad o en un pueblo de unas pocas docenas de habitantes. A mayor grado de conocimiento sobre uno, menor grado de libertad para desviarse de la norma tendrá. Cuando se sabe todo sobre ti terminas por ser como un coche de Scalextric, la única opción es circular por el carril.

La interactividad es otra de las características de las redes. Para eso están diseñadas, para que todo el mundo pueda comunicarse y responder. Pero la mente humana acepta mucho mejor las proposiciones en las que participa que aquellas que vienen de terceros. Una decisión consensuada en un "diálogo" se adopta como propia y se incorpora a las convicciones más profundas. Internet es una máquina perfecta de convencer. Por una parte, segmenta el discurso de forma interesada de modo que solo ves una parte de la realidad, por otra te implica en la discusión sobre el asunto del que se trate. El resultado final es que un instrumento diseñado para la transmisión de información de forma horizontal termina por hacerlo verticalmente, de arriba abajo.

La dependencia que los sistemas de mando y control militares actuales tienen de la tecnología hace que una interrupción de los servicios que se prestan a través de las redes digitales tenga el potencial de paralizar a un ejército

Esto último tiene dos matices. En primer lugar, la posibilidad de encontrar personas con pensamientos similares al tuyo con las que jamás hubieras coincidido en la vida física. Eso permite cooperación en investigación, pero también integración de minorías ideológicas o de cualquier tipo que pueden formar su "pandilla" a miles de kilómetros de distancia. Colectivos muy minoritarios encuentran apoyo en las redes, igual que radicalismos que jamás hubieran cuajado por la dispersión de sus miembros terminan por juntar una masa crítica suficiente con elementos dispersos.

El segundo matiz a la distribución vertical de la información —que llevaría a un adoctrinamiento— es la necesidad compulsiva que han introducido los dispositivos (especialmente los móviles) de consumo de noticias. Esta intoxicación de información, *infoxicación*, supone un bombardeo incesante de datos muchas veces no coherentes que no forman un relato. La consecuencia es la falta de elaboración de principios y valores, y la

posibilidad de contrarrestar casi cualquier información con una lluvia de desinformación que conduce a una anarquía y al desinterés general por la realidad.

La universalidad, interactividad, rapidez, movilidad y demás características de la Internet son cualitativamente distintas a lo que había antes de las redes. La seguridad, la privacidad y la libertad se ven afectadas por todas ellas y, por lo tanto, su naturaleza cambia con el cambio del entorno. La ciberseguridad no es otra cosa que la seguridad de siempre, pero entendiendo cuáles son las nuevas amenazas a la misma y las consecuencias de no proporcionarla. Estamos en un equivalente histórico —sinanimus exagerandi, como dirían Les Luthiers— al momento en que los peces abandonaron el medio acuático para vivir en tierra. Las nuevas condiciones llevan aparejada la necesidad de cambiar la forma en que respiramos y la dieta de la que nos alimentamos. Ha cambiado el ecosistema, no la necesidad de seguridad.

2 *Ciberguerra*

La definición de guerra implica un enfrentamiento entre Estados con el fin de imponer la voluntad de uno sobre el otro en el que se alcanza un determinado umbral de violencia. Tradicionalmente, este umbral se medía en un número de muertos o en un grado concreto de destrucción física. Si la guerra es la continuación de la política por otros medios, tendríamos que determinar si los medios cibernéticos pueden considerarse armas y, por lo tanto, dar lugar a un conflicto armado.

Pero este no es el momento ni el lugar para entrar en esos debates. Lo que es relevante es la capacidad de las herramientas cibernéticas para doblegar la voluntad de un adversario. En un mundo que Baumann describe como líquido, en un entorno bélico que empieza a describirse como "zona gris", en una geopolítica en la que los actores pueden o no ser estatales, lo que menos relevancia tiene es el tipo de instrumento que se emplee para obtener la victoria. Se emplean todos y cada uno de los disponibles, desde las sanciones económicas o industriales hasta el terrorismo o la invasión de un territorio por fuerzas mercenarias. El ciberespacio se ha convertido en una más de las formas de actuar en un conflicto.

Pero esta "zona gris" ya no se limita a tiempos en que los embajadores han arrojado sus guantes y declarado formalmente las hostilidades, ni se lucha en los campos de batalla mientras la población espera el resultado del combate desde las murallas de la ciudad. Hoy la guerra se libra EN la gente, dentro de cada uno de nosotros y de nuestros dispositivos, en nuestras cabezas y en nuestros corazones, y en los de nuestros avatares.

La guerra se ha trasladado a los relatos y las narrativas. A través del ciberespacio ha pasado al entorno cognitivo, a nuestro entendimiento y nuestros sentimientos. La guerra ya no es lo que era. O quizás ha pasado a serlo de una forma mucho más intensa. Los coroneles Qiao Liang y Wang Xiangsui lo anunciaban ya en 1999 en su "Guerra sin restricciones". Esa capilaridad que permite Internet, esa capacidad para llegar hasta el fondo de cada uno de nosotros, habilita también a los Estados a traer a guerra a nuestro interior. Y a los no-Estados.

Pero es importante recordar el carácter dual del ciberespacio como entorno y como herramienta también en la guerra. Las grandes potencias se aprestan a luchar en y con él en combinación con el armamento convencional y, si procede, el nuclear. La dependencia que los sistemas de mando y control militares actuales tienen de la tecnología hace que una interrupción de los servicios que se prestan a través de las redes digitales tenga el potencial de paralizar a un ejército.

Esta realidad se comprobó ya cuando Israel fue capaz de bombardear una central nuclear que Siria estaba construyendo en 2007 tras cegar a la defensa aérea siria con un ataque informático. En la actualidad, los planes de ataque incluyen el uso de submarinos especialmente diseñados para atacar los cables de fibra óptica que transitan por el fondo de los océanos, la explosión de artefactos nucleares para generar un pulso electromagnético que "fría" los sistemas de comunicaciones de los satélites, la activación de virus, gusanos y troyanos durmientes en las infraestructuras críticas del enemigo, o la saturación de la capacidad de respuesta de las páginas web.

Se trata de ataques cibernéticos sobre la misma estructura del ciberespacio, pero también sobre infraestructuras de comunicaciones, transporte, banca y finanzas, o servicios públicos. Todo lo que esté conectado o sea conectable, además de nosotros mismos como parte del mundo de la información, es susceptible de ser atacado.

Se cuenta la anécdota de que, preguntado por cómo iba a ser la Tercera Guerra Mundial, Einstein afirmó no saberlo, pero aseguró que la cuarta se pelearía con palos y piedras después de una catástrofe nuclear. El estado actual de la tecnología permite afirmar que esa guerra con palos y piedras empezará a los diez minutos de comenzar la tercera guerra. Y que será después de que hayamos perdido el acceso a todo aparato tecnológico después de la inutilización mutua de las redes informáticas de los contendientes y del resto del mundo.

Vivimos en el ciberespacio tanto como en el mundo físico. Somos anfibios entre dos mundos con reglas distintas. Todo lo bueno y malo que hay en nosotros se manifiesta en los dos, aunque de forma distinta, con herramientas diferentes y con consecuencias desiguales. La seguridad sigue estando en la base de nuestra pirámide y la guerra sigue siendo la cúspide de nuestra forma de enfrentarnos, pero ahora tenemos que entender ambas de un modo nuevo.

Yaiza Rubio

Analista de seguridad en ElevenPaths

Desde mayo de 2013 ejerce como analista de seguridad en ElevenPaths tras haberlo hecho en empresas como S21sec e Isdefe, además de ser colaboradora del Centro de Análisis y Prospectiva de la Guardia Civil y coautora del libro *Bitcoin: La tecnología blockchain y su investigación*.

Ha sido nombrada cibercooperante de honor por INCIBE (2017) y premiada como finalista de los Proyectos I+D+i del V Security Forum (2017), segundo premio del hackathon de INCIBE en el Mobile World Congress (2017), tercer premio de la Cátedra de Servicios de Inteligencia y Sistemas Democráticos (2015) y segundo premio del Reto de ISACA de jóvenes investigadores (2015). A nivel universitario, es docente en diferentes postgrados sobre análisis de inteligencia, seguridad, análisis forense, evidencia digital y fuentes abiertas, además de codirigir el Posgrado de experto en Bitcoin y Blockchain de la Universidad Europea de Madrid. En el ámbito técnico, se dedica a la publicación de contenidos científico-técnicos en eventos como Blackhat (2017), Defcon (2017), EuskalHack (2017), MaríaPitaDefcon (2017), ISMS Forum (2016), SummerBootcamp (2016), 8dot8 (2015), Cybercamp (2015 y 2017), NavajaNegra (2015), JNIC (2015) o RootedCon (2015), así como a la participación en numerosas jornadas de formación y concienciación en materia de ciberseguridad y privacidad.

Twitter: @yrubiosec

LOS CLAROSCUROS
de la ciberseguridad

Yaiza Rubio

Sin que se asemeje a una excusa, se torna realmente complicado sintetizar el complejo mundo de los riesgos de Internet y la evolución que está teniendo el sector de la ciberseguridad en un artículo que contiene menos de tres mil palabras. No por la cantidad de titulares pensados desde el *clickbaiting* cuyo efecto es el de aterrorizar al usuario medio de Internet, sino por la calidad y la cantidad de investigación existente sobre este campo que es la que hace que, un medio que no nació concebido desde la seguridad desde el diseño sino más bien el de ofrecer una vía adicional de comunicación a las que disponíamos y al que ha habido que ir implementando parches.

La situación actual no es tan dramática como se percibe desde fuera. Hasta hace bien poco las credenciales viajaban por la red en claro utilizando protocolos como HTTP. No existía la autenticación en dos pasos. No existía concienciación sobre la gravedad de un incidente. Antes, los sistemas estaban pensados para conectarse, no para ser seguros. Una frase que refleja esta situación es la que diría mi querida Mafalda: "No es cierto que todo tiempo pasado fue mejor. Lo que pasaba era que los que estaban peor todavía no se habían dado cuenta".

1 *Sobre la necesidad de ciberseguridad*

El concepto de ciberseguridad es muy amplio porque aplica a numerosos campos pero podría resumirse como la práctica de defender aquellos sistemas informáticos de ataques maliciosos. Uno de los principios más importantes de una estrategia defensiva efectiva es el de la *defensa en profundidad* definida por el Centro Criptológico Nacional (CCN-CERT) como la estrategia de protección consistente en introducir múltiples capas de seguridad que permitan reducir la probabilidad de compromiso en caso de que una de las capas falle y en el peor de los casos minimizar el impacto. De este principio se desprende una máxima del mundo de la seguridad: "La seguridad al 100 % no existe".

La exposición tecnológica de una determinada organización, así como la tecnología legada o el impacto de no proteger sus activos más valiosos como la

información de sus clientes, entre otras cosas, son desafíos frecuentes que hacen darnos cuenta de que el riesgo de recibir un determinado ataque no es el mismo para todas las organizaciones. El principio existente detrás de este concepto es el de dificultar las acciones del atacante a través de las diferentes medidas de seguridad aplicadas a cada una de las capas de forma que los diferentes sensores que tenga nuestro sistema detecten las actividades maliciosas. Cuando una capa se vea comprometida, las medidas de detección, de reacción y de recuperación nos permitirán reaccionar, disminuyendo la probabilidad de que otras capas se vean comprometidas. De esta manera, evitamos así que la seguridad del servicio en su conjunto se vea burlada, disminuyendo por tanto el riesgo.

La inversión que siguen actualmente las organizaciones se encuentra muy ligada a la correcta percepción sobre la gestión de sus riesgos. Es un error pensar que nunca va a ocurrir un desastre como el que viví y del que tanto aprendimos de Wannacry y que van a ser capaces de proteger sus sistemas ante cualquier ataque por lo que se trata de desarrollar políticas de ciberseguridad ligadas al negocio.

Las empresas medianamente maduras balancean sus presupuestos de seguridad entre soluciones de prevención y de detección realizando un análisis continuo de vulnerabilidades, monitorizando qué está pasando en su red identificando accesos no autorizados porque, sin duda alguna, en algún momento un ataque va a tener éxito. En cambio, las más maduras son las que se plantean qué van a hacer el día que tengan un fallo de seguridad, qué van hacer el día en el que un empleado se lleve información de la empresa o qué van a hacer el día en el que un ataque DDoS deje sin disponibilidad su web. En resumen, qué medidas van a tomar cuando el servicio que utilizan sus clientes siga funcionando.

2 Las diferentes visiones sobre la privacidad

Internet está siendo utilizado con éxito por grupos organizados para satisfacer sus objetivos pero serán las necesidades de cada grupo lo que marcará el tipo de aplicaciones o servicios que utilizarán para llevarlos a cabo. En este sentido, las organizaciones que centran sus esfuerzos en acciones de presión harán uso de la web de superficie (parte de Internet indexada por buscadores tradicionales) como blogs, redes sociales o plataformas de firmas para garantizar la difusión de su mensaje garantizándose su llegada a un público amplio. Por el contrario, aquellos grupos criminales o aquellas organizaciones que lleven a cabo actividades perseguidas por estados optarán por soluciones que provean una capa de anonimato más robusta (Tor, I2P, Freenet, etc.) para dificultar las labores de investigación de las agencias de seguridad.

La masacre de San Bernardino desató una guerra tanto legal como mediática entre gran parte de los fabricantes de tecnología y el FBI después de que Apple se opusiera fuertemente a liberar un iPhone propiedad de un presunto terrorista

En este sentido, la colaboración entre las fuerzas de seguridad y las principales empresas tecnológicas es crucial en cuanto a compartición de información se refiere. Los primeros tratan de hacer su trabajo con la dificultad que entrañan aquellos delitos que se comenten a través de la red o que se ha utilizado como herramienta para la comunicación. Y, algunos de los segundos, en aras de luchar por la privacidad de los usuarios se niegan a compartir su información. La masacre de San Bernardino desató una guerra tanto legal como mediática entre gran parte de los fabricantes de tecnología y el FBI después de que Apple se opusiera fuertemente a liberar un iPhone propiedad de un presunto terrorista.

En 2016, a raíz de aquello, algunos de los fabricantes comenzaron a tomar medidas para adecuarse a las necesidades de los nuevos tiempos en materia de privacidad. La implementación del cifrado punto a punto, como fue el caso de Whatsapp o el reporte periódico que hace Google sobre el número de peticiones de información sobre sus usuarios por parte de las Fuerzas y Cuerpos de Seguridad o el anuncio de la política de privacidad de Apple con el eslogan de fondo *What happens on your iPhone, stays on your iPhone* han sido algunas de ellas. A lo largo de 2018 con Facebook casi siempre en el foco de los escándalos de seguridad es cuando nos hemos dado cuenta que no era tan cierta la percepción que se tenía de que a los usuarios no les importa su privacidad.

El 25 de mayo de 2018 fue el día en el que comenzó a ser de obligado cumplimiento la GDPR donde se hace referencia a dos principios para la implementación efectiva de la responsabilidad proactiva como son los de protección de datos desde el diseño y protección de datos por defecto. El principio de protección de datos desde el diseño tiene como objetivo cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados

El director del FBI, James Comey, y la Fiscal General, Loretta Lynch, en la rueda de prensa sobre el titoreo masivo en San Bernardino / Foto: FBI

y busca que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto.

Pocas veces he visto a arquitectos o desarrolladores de software tan preocupados por comprender cada uno de los artículos donde se mencionan términos como "dato de carácter personal", "transparencia", "desde el diseño", "por defecto" o "tratamiento" para que la implementación esté realmente alineada con lo que pide la GDPR. Va a hacer un año desde que comencé a liderar un proyecto en la empresa donde trabajo actualmente que está íntimamente relacionado con uno de los proyectos IT con más envergadura que he visto, como es la Cuarta Plataforma.

Este proyecto fue diseñado para apoyar y cumplir plenamente con el espíritu y la letra de este reglamento introduciendo una serie de conceptos centrales para definir cómo manejar información personal permitiendo a su vez dotar de capacidades de gobierno de datos, control de acceso, registro y auditoría, entre otras.

Estos conceptos centrales son los llamados consentimientos (una acción explícita y voluntaria que el cliente realiza para permitir que se realice una acción por ejemplo una firma en un papel, una grabación de voz o un clic en el botón "Autorizar" de un sitio web), los propósitos (la razón por la que se desea procesar información personal. Por ejemplo, una aplicación puede querer manejar información personal para crear una recomendación de película para un cliente) o procesamiento de datos (almacenar, transformar o acceder a información personal se considera procesamiento de datos).

3 *La importancia de la colaboración*

La realidad es que la ciberseguridad no consiste solo en estar preparado a nivel individual. Es necesario implantar normas, políticas y establecer relaciones con otros organismos capacitados para tomar decisiones en todo el entorno para acotar el campo de actuación de aquellos que quieren aprovecharse de la situación. La ciberseguridad es una cuestión de carácter global que necesita de la colaboración de todos los países para hacer frente a los retos que se plantean.

En España, es el Consejo Nacional de Ciberseguridad es el encargado de reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privado tanto en el ámbito nacional como en el internacional. Como parte de este, el Instituto Nacional de Ciberseguridad de España (INCIBE), como sociedad dependiente del Ministerio de Economía y Empresa, a través de la Secretaría de Estado para el Avance Digital es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y

especialmente para sectores estratégicos contribuyendo así a construir ciberseguridad a nivel nacional e internacional.

Una de las relaciones centrales del Gobierno de España es la mantenida con la Organización de los Estados Americanos (OEA) bajo un acuerdo de colaboración para el desarrollo de diferentes acciones de cooperación que buscan reforzar los niveles de protección y resiliencia a nivel internacional. Algunas de las actividades llevadas a cabo han sido las siguientes:

- **International CyberEx:** consiste en la ejecución de un ciberejercicio virtual en donde se buscó fortalecer las capacidades de respuesta ante incidentes, así como una mejora de la colaboración y cooperación ante este tipo de incidentes en formato Capture The Flag (CTF). Este formato está basado en un modelo de competición de ciberseguridad diseñado para servir como un ejercicio de entrenamiento que permita otorgar a los participantes experiencia en el seguimiento de una intrusión, así como trabajar en las capacidades de reacción ante ciberataques análogos que sucedan en el mundo real.
- **Cybersecurity Summer BootCamp:** un programa de capacitación especializado en ciberseguridad dirigido a personal técnico que trabaje en Centros de Respuesta a Incidentes (CERTs o CSIRTs), miembros de Fuerzas y Cuerpos de Seguridad que trabajen en unidades operativas relacionadas con la ciberseguridad y personal en activo perteneciente a las carreras judicial o fiscal, abogacía del Estado, funcionarios de la Administración de Justicia y personal de organismos reguladores o legislativos que trabajen en áreas relacionadas con los aspectos jurídicos y normativos de la ciberseguridad.
- **Ibero-American Cybersecurity Challenge (ICSC):** el objetivo de esta iniciativa internacional es fomentar el talento en ciberseguridad y animar a los jóvenes a seguir una carrera técnica profesional en un sector con gran demanda y oportunidades, además de promover el conocimiento, el liderazgo y el fortalecimiento de las relaciones entre los países participantes.
- **Foro Internacional de Género y Ciberseguridad:** sus objetivos principales son el de promover el intercambio de información y el desarrollo de conocimientos sobre género y ciberseguridad, analizar la situación actual y problemática de género tanto a nivel nacional como internacional en relación al sector de la ciberseguridad y debatir sobre los principales problemas en relación a la violencia de género en el ámbito digital.

Actualmente, España ocupa el puesto quinto y séptimo a nivel europeo e internacional, respectivamente, en el Índice Global de Ciberseguridad que labora la ITU, un organismo de las Naciones Unidas que se centra en las

Tecnologías de la Información y la Comunicación. Cada año realiza una encuesta que mide el compromiso de los Estados Miembros con la ciberseguridad y que muestra cómo España está por encima de otros países europeos en este ámbito.

4 De profesión hacker

No solo ha ido cambiando la percepción de los conceptos de privacidad y seguridad, sino también las profesiones que se necesitan para llevar a cabo el cambio. El proceso que estamos presenciando sobre la digitalización de las compañías está llevando a un crecimiento de ofertas laborales solicitando perfiles bajo el título de analistas en ciberseguridad. Enmascarado bajo este formalismo, se encuentra la filosofía de la profesión del hacker.

El término 'hacker' no es algo nuevo. En realidad, fue definido en 1993 en un glosario realizado por el Grupo de Trabajo de Ingeniería de Internet (IETF). Ellos los definieron como aquella persona que se deleita en tener una comprensión íntima del funcionamiento interno de un sistema, de los ordenadores y de las redes informáticas en particular.

Esta inquietud por saber cómo funcionan los sistemas tiene un trasfondo muy lejos del estereotipo que se ha proyectado desde hace unos años en los medios de comunicación. El fin último de estas personas es hacer de Internet un mundo mucho más seguro, tanto para las compañías, organismos públicos o cualquier usuario que vaya a hacer uso de él. Sin embargo, el término es a menudo mal utilizado en un contexto peyorativo, donde cracker (o cibercriminal) sería el término correcto. Al final, un conocimiento tan profundo sobre una tecnología puede también ser utilizado con fines maliciosos llegando incluso a paralizar empresas por completo como fue el sonado caso de WannaCry.

Principalmente durante días como esos, es cuando las empresas que han invertido en seguridad y en este tipo de perfiles tienen que demostrar el nivel de madurez que han alcanzado y responder así a lo que está sucediendo sin apenas información. No solamente para identificar cuanto antes dónde se encuentra el problema y así dejar de ser vulnerables, sino también para compartir el conocimiento adquirido con el resto de compañías y organismos públicos para evitar que también lo sean.

Además de ese sentimiento por compartir, también les caracteriza el de ayudar a los demás. Comparten lo que saben de una forma completamente altruista cuyo único objetivo es concienciar a aquellos segmentos de la población que pudieran no estar tan concienciados con los riesgos que conlleva Internet. Una mínima formación en seguridad entre los más pequeños y su entorno, es ya esencial en un mundo que tiene los vestigios de convertirse completamente digital.

El término hacker no es algo nuevo. En realidad, fue definido en 1993 en un glosario realizado por el Grupo de Trabajo de Ingeniería de Internet (IETF). 'Hacker' es a menudo es un término mal utilizado en un contexto peyorativo, donde 'cracker' (o 'cibercriminal') sería el término correcto

Este tipo de proyectos que llegan a todo el mundo también sirven para visibilizar y hacer más atractivo el sector de la seguridad inculcándoles que no es una profesión imposible de acceder y que no es una profesión únicamente de hombres. Es importante que comencemos a cambiar entre todos el estereotipo impuesto en el pasado sobre el perfil del hacker para que nadie se quede fuera a la hora de elegir profesiones técnicas a las que dedicarse.
En conclusión, qué voy a decir yo, mi profesión mola. Tiene retos constantes cuyos días son muy diferentes, pero en mi opinión quizá lo más importante sea el poder que tenemos a día de hoy de abrir los ojos a la sociedad dando a conocer que no es cierto que todo tiempo pasado fue mejor. Si tuviera que elegir un momento de la historia para nacer y no supiera de antemano quién sería yo también elegiría el presente.

Pedro Pacheco

Es licenciado en Derecho y también en Ciencias Policiales por la Universidad de Salamanca. Forma parte del Cuerpo Nacional de Policía desde hace 26 años, siempre en el área de Policía Judicial.

Entre los años 1996 y 1998, fue Inspector, Jefe del Grupo de Policía Judicial en la Comisaría de Tenerife. Después de esto y hasta el año 2009, fue Inspector, Jefe del Grupo de Crimen Organizado de Madrid. En el centro de Madrid, desde 2009 hasta 2015, fue Inspector Jefe, Jefe de la Sección de Policía Judicial. Durante los dos años siguientes, de 2015 a 2017, fue Inspector Jefe, Jefe de Homicidios de Madrid. Desde entonces y hasta la actualidad, es Comisario Jefe de la Brigada Central de Investigación Tecnológica.

Comisario Jefe de la Unidad Central de Ciberdelincuencia de la Policía Nacional.

Twitter: @policía

CIBERDELINCUENCIA EN ESPAÑA

Un desafío para el Cuerpo Nacional de Policía

Pedro Pacheco

La ciberdelincuencia, igual que ocurre con la ciberseguridad son conceptos que de un tiempo a esta parte han pasado de ser prácticamente desconocidos para la sociedad en general a adquirir una transcendencia que podría ser calificada de notoria.

Y si bien es cierto que ciberdelincuencia y ciberseguridad son cosas diferentes también lo es que tienen muchos aspectos en común, por ejemplo que el gran protagonismo que han venido adquiriendo está estrechamente ligado a la espectacular implantación que en los últimos años han tenido en nuestras vidas las nuevas tecnologías, especialmente las tecnologías de comunicación e información, comúnmente conocidas como TIC.

Y digo últimos años, porque por ejemplo Internet (sin duda la más conocida e implantada de las nuevas tecnologías) hace apenas cuatro décadas era un mero proyecto, que ha venido evolucionando a pasos agigantados hasta llegar al día de hoy, al presente, en el que estamos hablando de inteligencia artificial, 5G o del Internet de las cosas, es decir el Internet que se integra y lo domina todo, de manera tal que desde un simple teléfono móvil que todos llevamos encima somos capaces de controlar la mayoría de los aspectos de nuestras vidas, desde el correo electrónico, pasando por las alarmas de las casas, el contacto con los profesores de los hijos, la ubicación de nuestros coches, por no hablar de la adquisición de cualquier tipo de producto, etc.

Y si hablamos del ámbito físico o territorial, el auge de las nuevas tecnologías no se circunscribe a determinados lugares del planeta como por ejemplo las zonas más desarrolladas o ricas, sino que su implantación ha sido global, es decir afecta a todo el mundo. Sirva de ejemplo lo que a diario comprueban los policías de fronteras con los inmigrantes que tratan de acceder a España procedentes de zonas tremendamente pobres, y que carecen absolutamente de todo, y su única posesión se ciñe a la ropa que traen puesta y los terminales telefónicos que prácticamente todos ellos portan.

De la confluencia de estos dos ámbitos (temporal y territorial), y unido a la circunstancia que la implantación de las TIC afecta a todas los entornos que conforman el comportamiento humano: cultural, económico, social, laboral, doméstico, etc., podemos aseverar que se ha generado un cambio transcendental en la manera en que nos relacionamos y entendemos el mundo, a lo que coloquialmente se le define como la revolución tecnológica.

Esta revolución de las nuevas tecnologías nos está aportando mayoritariamente cosas buenas, nos está haciendo la vida más cómoda, y nos está generando una calidad de vida que hace unos años era impensable.

Aunque también estamos comprobando que no todo es positivo; también hay un lado negativo, que un número considerable de nuestros conciudadanos se

están valiendo del avance de la tecnología para llevar a cabo actividades delictivas, entrando en el campo de la ciberdelincuencia y los ciberdelincuentes.

En las próximas líneas voy a procurar dar una visión completa de la ciberdelincuencia en España, desde el punto de vista policial fundamentalmente, y para ello, en primer lugar se va a mostrar cuál es la situación real en cifras de la cibercriminalidad en España, es decir los delitos totales que se cometen en el país, para a continuación exponer la respuesta estratégica que ofrece el Cuerpo Nacional de Policía a esa ilícita actividad.

1 *La ciberdelincuencia en España. Cifras*

Antes, es preciso definir qué entendemos por ciberdelincuencia, y si bien es cierto que tradicionalmente se ha asimilado el ciberdelito a aquellos ilícitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos, tales como ataques o intrusiones informáticas, denegaciones de servicio, etc. (comúnmente conocidos como delitos de *hacker*), actualmente y debido al avance de esta modalidad delictiva, al hablar de ciberdelincuencia debemos entenderla en un sentido amplio, es decir, todos aquellos delitos que para su comisión el autor o autores se valen del empleo de las nuevas tecnologías.

Precisando, que si bien es cierto que en este concepto se incluye la comisión de delitos mediante el empleo de sistemas físicos o analógicos (lectores de tarjetas, microcámaras espía, grabadoras, etc.), la gran mayoría de estos hechos ilícitos en la actualidad son cometidos a través de Internet.

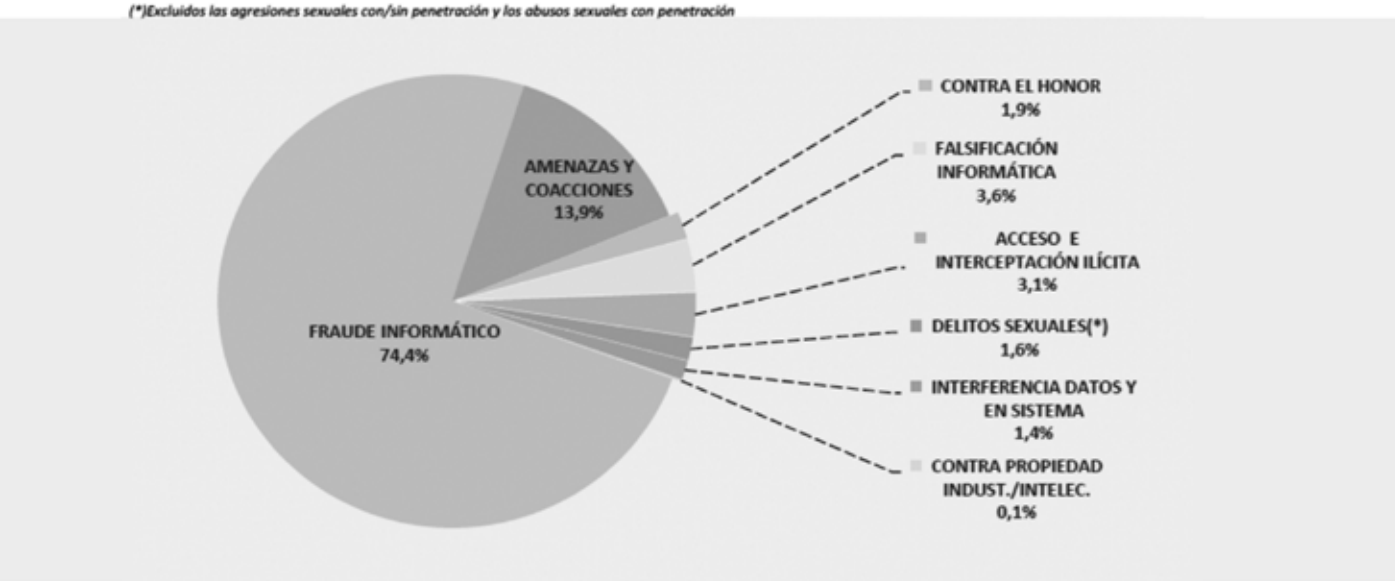
Partiendo de este concepto amplio, en la siguiente imagen se muestra la realidad de la ciberdelincuencia en España. Estos datos se han extraído del informe de cibercriminalidad elaborado anualmente por la Secretaría de Estado de Seguridad, dependiente del Ministerio del Interior, y muestra por años los hechos conocidos (denuncias de ciudadanos más la suma de las actuaciones policiales) en territorio de Policía Nacional y Guardia Civil desde el año 2014 al 2017, significando que el informe de el año 2018 al día de elaboración del presente aún no se había publicado.

La tabla inferior (circular) nos muestra los datos porcentuales sobre el total de cada uno de los diferentes delitos tecnológicos, siendo de destacar el fraude informático, que supone el 74,4 por ciento del total.

La primera tabla muestra tanto el número total de hechos de todos los delitos que pueden ser cometidos a través de las nuevas tecnologías como el cómputo global de todos ellos por años.

HECHOS CONOCIDOS	2014	2015	2016	2017
ACCESO E INTERCEPTACIÓN ILÍCITA	1.851	2.386	2.579	2.505
AMENAZAS Y COACCIONES	9.559	10.112	11.473	11.270
CONTRA EL HONOR	2.212	2.131	1.524	1.537
CONTRA PROPIEDAD INDUST./INTELEC.	183	167	121	109
DELITOS SEXUALES(*)	974	1.233	1.188	1.312
FALSIFICACIÓN INFORMÁTICA	1.874	2.361	2.697	2.961
FRAUDE INFORMÁTICO	32.842	40.864	45.894	60.511
INTERFERENCIA DATOS Y EN SISTEMA	440	900	1.110	1.102
Total HECHOS CONOCIDOS	49.935	60.154	66.586	81.307

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



Lo más importante, desde el punto de vista policial, es observar las tendencias que se registran año tras año, pudiéndose comprobar cómo en los últimos años en España la delincuencia tecnológica viene aumentando en torno a un 14 por ciento anual, señalando que esta tendencia de incremento se ha mantenido durante todo el año 2018 y los cinco primeros meses de 2019.

Es preciso significar que los delitos que no requieren para su ejecución el empleo de tecnología, llamémoslos "tradicionales", especialmente los del orden socioeconómico, viene sucediendo todo lo contrario, en los últimos años tienden a mantenerse o disminuir, lo que significa que estamos siendo testigos de un cambio de tendencia en la criminalidad a favor de la delincuencia tecnológica.

2 *Estrategia del Cuerpo Nacional de Policía*

En base a los datos expuestos, nos podemos preguntar qué tipo de respuesta ofrece el Cuerpo Nacional de Policía a sus ciudadanos para hacer frente a este incremento de hechos y al desafío que empieza a suponer la ciberdelincuencia.

Para dar respuesta a esta cuestión se debe hacer mención al Plan Estratégico Institucional (PEI) elaborado por la Dirección General de la Policía para el periodo 2017-2021 en el que se definen cuáles son los grandes objetivos que se pretenden conseguir por la institución policial en ese periodo de tiempo.

Este PEI además de considerar la lucha contra la ciberdelincuencia como un área prioritaria de actuación, lo incluye como uno de los grandes objetivos estratégicos con la siguiente definición: "Prevenir y luchar contra la Ciberdelincuencia potenciando la ciberseguridad", que a su vez se concreta en tres objetivos específicos:

1. Detectar las amenazas y vulnerabilidades de los sistemas informáticos
2. Potenciar la atención al ciudadano, prestando especial atención a las redes sociales y a la lucha contra la explotación sexual infantil
3. Luchar contra el fraude en Internet

La Unidad encargada de hacer cumplir estos objetivos es la Unidad Central de Ciberdelincuencia, encuadrada dentro de la Comisaría General de Policía Judicial y que presenta la siguiente estructura:

Esta unidad, dentro del Cuerpo Nacional de Policía, es la competente para llevar a cabo la investigación y persecución de las actividades delictivas que impliquen la utilización de las tecnologías de la información y la comunicación (TIC) y el ciberdelito de ámbito nacional y transnacional, y está compuesta de tres brigadas:

1. Brigada de Seguridad Informática

Es la encargada de cumplir el primer objetivo: detectar las amenazas y vulnerabilidades de los sistemas informáticos.

Las investigaciones que desarrolla esta brigada están relacionadas con la ciberseguridad, ataques informáticos a sistemas de información y telecomunicaciones cometidos por personas u organizaciones criminales valiéndose de medios técnicos avanzados y que pretendan cualquier objetivo, fundamentalmente el patrimonial.

Tipología penal: ataques o daños informáticos, denegaciones de servicio distribuido (Ddos), malware, distribución ilícita de señal a través de sistemas de *Cardsharing*, IPTV, OTT streaming. También investigaciones relacionadas con divisas virtuales y criptomonedas: seguimiento de transferencias en *blockchain*, de *exchangers*, *mixers*, etc.; seguimiento de divisas virtuales usadas e interacción entre las mismas.

Es una brigada transcendental, pues esta actividad delictiva tiene la virtualidad que un único sujeto activo (autor) puede causar miles y miles de víctimas e incluso causar desestabilizaciones de instituciones.

Sirva como ejemplo de la actividad desarrollada por los componentes de esta brigada una investigación, la Operación Carbanak, culminada el año pasado, y en la que contamos con el apoyo operativo del FBI norteamericano, en la que fue detenido uno de los más importantes cibercriminales de la historia, Denis T., asentado en España, líder de una organización internacional, especializada en la creación de un tipo de *malware* que una vez introducido en los servidores informáticos de las entidades bancarias conseguían tomar el control de los sistemas críticos del banco. Esto les permitía alterar saldos de cuentas controladas por la organización; modificar cuentas destinatarias en transferencias de alto valor, o directamente gestionar de forma remota los cajeros automáticos para vaciarlos. La organización criminal consiguió a lo largo de su actividad tomar el control de la red de un número considerable de bancos de ubicados tanto en Rusia, como en las antiguas repúblicas de la

Unión Soviética, calculándose que los beneficios obtenidos por estas sustracciones pudieran superar los mil millones de dólares. Las ganancias de cada ataque, que superaban el millón y medio de dólares como media, eran convertidas inmediatamente en criptomonedas (especialmente *bitcoins*) para facilitar su movimiento en una red internacional de blanqueo de capitales.

Es preciso señalar, que esta práctica de convertir el dinero monetario en dinero virtual o criptomoneda se está convirtiendo en los últimos meses en algo habitual entre las organizaciones criminales dedicadas a estos sofisticados ilícitos, todo ello con el fin de dificultar el rastreo policial del dinero, pues a diferencia de lo que sucede en una cuenta corriente bancaria, que va asociada a una numeración, en las criptomonedas lo que ocurre es que cualquiera puede generarse su propio número de cuenta, con el hándicaps que estas cuentas son aleatorias y no se puede predecir de antemano, ni conocer a que persona están asociadas. Su funcionamiento se basa en un sistema criptográfico público/privado que garantiza el anonimato de la persona que tiene el acceso a esa dirección y que puede gestionar el monedero virtual.

2. Brigada de Investigación Tecnológica

Esta brigada es la competente para aplicar el segundo objetivo: potenciar la atención al ciudadano, prestando especial atención a las redes sociales y a la lucha contra la explotación sexual infantil.

Si el primer objetivo específico se refería a la ciberseguridad y al ciberespacio, este segundo está claramente orientado a los internautas, a la seguridad de las personas en sus interacciones más comunes y en la protección de los más débiles.

Tipología penal: delitos contra la libertad sexual de menores de edad a través de Internet, pornografía infantil, corrupción de menores, sextorsión, *sexting*, ciberengaño pederasta o *child grooming*, acoso, extorsiones, amenazas, coacciones, delitos de odio, tráfico de medicamentos, etc.

Uno de los cometidos prioritarios de esta brigada es la lucha contra la explotación sexual infantil a través de Internet, concretándose sus investigaciones tanto en tratar de localizar los centros de producción de pornografía infantil, como en tratar de detectar la distribución de pornografía a través de la red, cuyos autores por norma general no tienen conexión entre sí, sino que intercambian archivos a través de grupos privados en multitud de plataformas y canales privados en redes sociales o bien mediante programas de intercambio tipo *peer to peer*.

De la experiencia adquirida en el desarrollo de investigaciones en la que los sujetos pasivos o víctimas son menores de edad, se puede concluir que en esta nueva realidad que es Internet y la ciberdelincuencia, si hay un sector social vulnerable en el que se ceban las nuevas formas de comisión de delitos es el de los menores, muchos de ellos ya "nativos digitales", y a pesar de ello o quizás por ello son objetivo de los delincuentes que se esconden tras las redes sociales, en un porcentaje notable con intenciones de índole sexual.

Uno de los cometidos prioritarios de esta brigada es la lucha contra la explotación sexual infantil a través de Internet, concretándose sus investigaciones tanto en tratar de localizar los centros de producción de pornografía infantil, como en tratar de detectar la distribución de pornografía a través de la red

Ante lo expuesto, surge la pregunta ¿existe un perfil de depredador sexual pedófilo en Internet? A lo que cabe responder que en base a la información obtenida en las múltiples investigaciones desarrolladas a lo largo de los años, se puede afirmar que no existe un perfil psicológico específico del pedófilo que actúa en Internet. No existen tramos de edad, antecedentes penales previos, patologías psicológicas o cualquier otra característica que permita diferenciarlos de las demás personas.

Podríamos decir que, por regla general, se trata de personas normales, cuya única diferencia es que el objeto de su deseo sexual reside en los niños y cuya satisfacción se realiza en su ámbito más personal e íntimo, su casa, y a través de un medio que permite su separación respecto a las víctimas, Internet.

Otra de las funciones encomendadas a esta brigada es la continua navegación y presencia en la red para detectar nuevos *modus operandi* y monitorización de posibles actividades ilegales para su consiguiente investigación, así como el control, seguimiento y análisis preventivo de los contenidos publicados en Internet, especialmente en redes sociales.

Policialmente se conoce esta actividad como ciberpatrullaje. Los agentes la llevan a cabo tanto en la web pública como en la *Dark Web*. En la primera, quedan registrados nuestros datos de conexión a través de la IP que nos asignan las proveedoras. Por otro lado, la *Dark Web* es la red no pública en la que los usuarios pueden navegar de manera anónima, sin que se registren sus datos de conexión. Para acceder a esta se requiere de unos navegadores específicos, siendo el más utilizado el denominado Red TOR (The Onion Router) cuya característica principal es que cifra y encripta las comunicaciones y oculta los números IP de identificación de los terminales.

Este anonimato conlleva que sea utilizado por la delincuencia para llevar a cabo todo tipo de acciones delictivas y de ahí la transcendencia del control policial.

3. Brigada de Fraudes Informáticos

Es la competente para tratar de cumplir el tercer objetivo: luchar contra el fraude en Internet (intensificar la respuesta policial sobre las estafas cometidas a través de las TIC).

Este objetivo específico está orientado a la actividad económica y a la industria financiera; al mantenimiento y protección del patrimonio y la investigación de todos los delitos contra el orden socioeconómico cometidos tanto a través de Internet como a través de las nuevas tecnologías. Si bien es cierto, como se ha podido constatar, que el aumento de los delitos tecnológicos afecta absolutamente a todos los bienes jurídicos protegidos (que sean susceptibles de ejecución a través de las nuevas tecnologías), es especialmente significativo en los delitos contra el patrimonio, pues suponen aproximadamente el 75% de todos los delitos denunciados.

Con respecto a los mencionados delitos contra el patrimonio, los mismos mayoritariamente se corresponden con fraudes o estafas cometidos a través de Internet, de los que el 70 % aproximadamente de los hechos se corresponden con el delito de *carding*, así denominado al uso ilegítimo de las tarjetas de crédito o débito titularidad de otras personas con el fin de obtener productos o dinero fraudulentamente. Las víctimas o perjudicados denuncian los cargos no autorizados por ellos que, mayoritariamente, son compras realizadas a través de páginas webs ubicadas en países extranjeros.

Significa que para llevar a cabo este tipo de estafas los delincuentes necesitan tener los datos contenidos en las tarjetas de créditos, los cuales son obtenidos bien mediante clonaciones físicas de las tarjetas en cajeros automáticos (*skimming*) o establecimientos comerciales, bien mediante las clonaciones virtuales de las tarjetas cuando se realizan compras a través de Internet en páginas poco seguras, bien obtenidos mediante *phising* (suplantación de empresas o personas para conseguir los datos bancarios de la víctima), o bien mediante ciberataques a los servidores o bases de datos de empresas donde se guardan datos de los clientes.

El ciberpatrullaje se lleva a cabo tanto en la web pública como en la Dark Web. En la primera, quedan registrados nuestros datos de conexión a través de la IP que nos asignan las proveedoras. Por otro lado, la Dark Web *es la red no pública en la que los usuarios pueden navegar de manera anónima sin que se registren sus datos de conexión. Para acceder a esta se requiere de unos navegadores específicos.*

Otro 15 % aproximadamente de los hechos se correspondería con estafas en compras o ventas de todo tipo de productos en páginas especializadas, entre los que se incluyen entradas a conciertos o eventos deportivos a través de Internet, productos de segunda mano, etc.

Y el 15 % restante aproximadamente, se correspondería con un conglomerado de fraudes que tienen como eje común el engaño a las víctimas y entre las que cabe destacar las estafas en alquileres, normalmente vacacionales, de inmuebles anunciados en páginas web creadas por los estafadores con un diseño web similar a otras de reconocida solvencia que inducen a error a los usuarios. Destacan también los conocidos como *Fraudes del CEO,* en los que los ciberdelincuentes se hacen pasar por un alto cargo de la empresa que pretende estafar; contactan, generalmente vía correo electrónico, con un empleado cualificado de la organización con la capacidad necesaria para hacer trasferencias o pagos importantes, y lo engañan para efectuarlo.

3 *Implantación de una cultura de la ciberseguridad*

No me gustaría finalizar el presente artículo sin dejar de mencionar como desde Policía Nacional, ante el desafío que supone el auge de la ciberdelincuencia, no solamente se están adoptando medidas de carácter operativo, como las hasta aquí plasmadas, sino que también se están llevando a cabo otras de carácter preventivo, que consisten en tratar de aconsejar e incluso educar a los ciudadanos de los riesgos asociados al uso de las nuevas tecnologías, bien a través de los exitosos perfiles institucionales creados por Policía Nacional en las más conocidas redes sociales, bien a través de las charlas y seminarios en materia de ciberseguridad impartidos en todos y cada uno de los centros educativos de nuestra jurisdicción, bien a través de cualquier tipo de foro que nos haga llegar al más amplio espectro de la sociedad.

Todo ello con el fin de tratar de implantar en la ciudadanía una cultura de la ciberseguridad, asumiendo que es un problema que requiere de una respuesta integral por parte de todas las administraciones, no solo de carácter policial, desarrollando políticas de prevención, incluso desde el inicio de su periplo formativo en la escuela, ya que se está manifestando un uso generalizado, poco responsable, de las tecnologías de la información y la comunicación.

Concluir mencionando las excelentes relaciones que mantiene el Cuerpo Nacional de Policía con las diferentes agencias de investigación norteamericanas, especialmente con el FBI a través de sus enlaces de la embajada norteamericana en Madrid. Son diversas las áreas de ciberdelincuencia en la que colaboramos habitualmente, pero posiblemente por su transcendencia cabe mencionar dos, los delitos vinculados con la ciberseguridad y los relacionados con la pornografía infantil, significando que las más transcendentales compañías tecnológicas y proveedores de Internet son estadounidenses y se rigen por tanto por leyes de aquel país, resultando fundamental para poder culminar con éxito las investigaciones relacionadas con las nuevas tecnologías esta excelente armonía policial.

Sigue la actualidad norteamericana a través de nuestro

Blog Diálogo Atlántico

#DiálogoAtlántico

Redes Sociales

El Instituto Franklin-UAH está presente en las siguientes redes sociales

Instituto Franklin-UAH

@IB_Franklin

Instituto Franklin-UAH

InstitutoFranklin

#TribunaNorteamericana, #TN

Los Estudios Norteamericanos en España a un clic

Suscríbete a nuestro boletín semanal

Para estar informado de las publicaciones, eventos, noticias, programas de estudios y otras oportunidades para investigar sobre Norteamérica y visitar Estados Unidos a través de becas y ayudas.

institutofranklin.net

Departamento de Comunicación
Responsable de Comunicación: Ana Lariño / ana.larino@institutofranklin.net
91 885 52 53 / 637 56 73 56

Tribuna Norteamericana

Tribuna Norteamericana está disponible para su descarga en PDF en la página web del Instituto Franklin: **www.institutofranklin.net**

La revista *Tribuna Norteamericana* es una publicación de difusión con base científica que recoge artículos relacionados con la política, la economía, la sociedad y la cultura de Estados Unidos. Cada número está dedicado a una temática y cuenta con colaboradores del ámbito de la diplomacia, la empresa, los medios de comunicación y la academia. Se distribuye en papel entre instituciones españolas y estadounidenses fuera y dentro de España, así como entre medios de comunicación y empresas.

La Fundación Consejo España-Estados Unidos colabora con *Tribuna Norteamericana*. De esta forma, la revista incluye una sección que lleva por título "La historia de" y que narra la experiencia de una empresa española (patrona de la Fundación) en EE. UU.

NÚMEROS ANTERIORES

Nº1. Mayo 2009
»The 2008 Presidential Election in Historical Perspective.
Andrew Richards

Nº4. Mayo 2010
»Las relaciones entre EE.UU. y Pakistán. Continuidad y cambio con la Administración Obama. Alberto Priego

Nº2. Octubre 2009
»Crusader America: Democratic Imperialism under Wilson and Bush.
Omar G. Encarnación

Nº5. Noviembre 2010
»The United States Supreme Court and the Political Process: The Contemporary Status of Voting Rights Law
Mark Rush

Nº3. Marzo 2010
»Política Hispana: España y las Comunidades Hispanas de Estados Unidos.
Guillermo López Gallego

Nº6. Abril 2011
»Un republicano en la Moncloa: la visita de Ronald Reagan a la España de 1985
Coral Morera Hernández

Nº7. Julio 2011

»El servicio diplomático norteamericano: el Foreign Service (FS).
Alberto Priego

Nº11. Enero 2013

» El difícil cambio de Obama hacia una histórica reelección
Dori Toribio
» Obama, "Cuatro años más"
Esteban López-Escobar
» Obama: del icono al poder de la imagen
Antoni Gutiérrez Rubí
» Obama "Forward"

Nº8. Marzo 2012

»Running for President, la ambición política y la influencia de los medios.
Vicente Vallés
»Barack Obama y su carrera política.
Roberto Izurieta
»Los efectos de la "americanización" de las campañas electorales del mundo.
Roberto Rodríguez Andrés

Nº12. Abril 2013

» Cómo los vemos y cómo nos ven
Inocencio Arias
» Las fronteras difusas del mercado en EE.UU.
David Fernández Vítores
» El factor hispano: cantidades, cualidades y debates
Francisco Moreno Fernández

Nº9. Julio 2012

»España y los hispanos en los EE.UU.: una llamada a la realidad.
Javier Rupérez
» ¿Qué significa ser Hispano en los EE.UU.?.
Octavio Hinojosa
»Estereotipo en el momento del cambio.
Emili J. Blasco

Nº13. Junio 2013

» U.S. Immigration Policy Debate, an investment in the future, or more roadblocks ahead?
Clara del Villar
» Hacia un nuevo modelo migratorio en EE.UU.
Secundino Valladares
» El impacto de la reforma migratoria en la economía de los EE.UU.
Eva Pareja

Nº10. Noviembre 2012

» La dura factura de la crisis sobre la imagen española en los EE.UU.
Pablo Pardo
» Claves para una Política Hispana: cómo fortalecer el papel de España en EE.UU.
Daniel Ureña
»España-Estados Unidos. Una relación de futuro
Gustavo Palomares

Nº14. Octubre 2013

» Los Foros España-EE.UU.
D. José Manuel García-Margallo
» Diplomacia pública y sociedad civil: la Fundación Consejo España-EE.UU.
Emilio Cassinello
» El Foro y el Consejo España-EE.UU.: los primeros años
Jaime Carvajal
» Dos décadas acercando sociedades
Juan Rodríguez Inciarte
» España-EE.UU.: medio milenio de historia común
Gonzalo de Benito
España-EE.UU.: una relación de futuro
Antonio Fernández-Martos Montero
» Panorama interdisciplinario del español en los EE.UU.
Francisco Moreno Fernández

Nº15. Abril 2014

» Cómo fomenta la diplomacia de EE.UU. la igualdad de género y la participación en política de las mujeres
Kate Marie Byrnes
» Women's Progress on the Road to Congress: A Comparative Look at Spain and the U.S.
Alana Moceri
» U.S. Latinas and Political Leadership
Lisa J. Pino
» ¿Imparable Hillary Clinton 2016?
Dori Toribio

Nº16. Septiembre 2014

» Ferrovial en EE.UU.: diez años haciendo camino
Joaquín Ayuso
» EE.UU. vs Europa: Distintos lenguajes, similar semántica
Sinuhé Arroyo
» Inbenta, el Google español
Julio Prada

Nº17. Enero 2015

» La historia de... Grifols en EE.UU. Greg Rich
» El posicionamiento del Reino de España ante el fracking... ¿ofrece datos relevantes la experiencia norteamericana?
Enrique Alonso
» Fracking, the Natural Gas Economy, and the Emerging US Industrial Renaissance
James Levy
» "¡Perfora, Sarah, perfora!" Manuel Peinado Lorca

Nº18. Abril 2015

» Diálogo Atlántico Varios autores

Nº19. Junio 2015

» La historia de... BBVA, un reto del siglo XXI: hacia la vanguardia digital
Juan Urquiola
» Un buen debate electoral
Dori Toribio
» American Political Campaigns: Costs, Techniques, & Technology
John Hudak
» El arte de hacer campaña en España y EE.UU.: ventajas y similitudes
Daniel Ureña

Nº20. Diciembre 2015

» La incipiente y aún borrosa Marca España en USA
Inocencio Arias
» Trabajando para afianzar la imagen de las empresas españolas en EE.UU. Alicia Montalvo Santamaría
» Un año especialmente fructífero en las relaciones entre España y EE.UU. Fidel Sendagorta
» La Comisión Nacional para las Conmemoraciones de la Nueva Es- paña: la historia que nos une José Manuel Ramírez Arrazola

Nº21. Marzo 2016

» La historia de... Repsol en Estados Unidos
Arturo Gonzalo Aizpiri
» Los nuevos fenómenos del terrorismo transnacional y la cooperación antiterrorista
Emilio Sánchez de Rojas Díaz
» Una aproximación a los acuerdos entre España y EE.UU.
Federico Aznar Fernández-Montesinos
» Hacia una nueva cooperación entre servicios de inteligencia
Julia Pulido Grager

Nº22. Junio 2016

» La historia de... El Instituto Cervantes en los EE.UU.
Ignacio Olmos
» El español en el sistema educativo de los Estados Unidos
Francisco Moreno Fernández
» El español en las redes sociales a través de la Embajada Española en Estados Unidos
Gregorio Laso
» El español en las campañas presidenciales de Estados Unidos
Daniel Ureña
» Entrevista a Jaime Ojeda
Manuel Iglesias Cavicchioli

Nº23. Noviembre 2016

» La historia de... Cosentino
Álvaro de la Haza
» Empresa y cultura, EE. UU. y España, una historia de éxito
Julia Sánchez Abeal
» Responsabilidad social corporativa, a uno y otro lado del Atlántico
Mercedes Temboury
» La sociedad, primera beneficiada del emprendimiento de alto impacto
Adrián García-Aranyos
» Un nuevo marketing para nuevas necesidades
Javier Iturralde de Bracamonte

Nº24. Junio 2017

» La historia de... Acciona en EE. UU.
Joaquín Mollinedo
» Donald J. Trump y el mundo: una relación conflictiva
Javier Rupérez
» El impeachment latente
Vicente Vallés
» El menguante círculo de confianza de Trump
Dori Toribio
» Todos los generales del presidente *Pedro Rodríguez*
» Perspectivas de las relaciones EE.UU.-RUSIA en la Administración Trump
Javier Morales

Nº25. Octubre 2017

» Trump, un OVNI inesperado
Inocencio Arias
» La OTAN y los EE.UU.: un futuro oscuro
Alberto Priego
» Trump y una América Latina en transformación: de la política de muro a la estrategia de sustitución Gustavo Palomares Lerma
» Trump 2.0 y Rusia en un teatro multipolar con sombras chinescas Rubén Ruiz Ramas

Nº26. Enero 2018

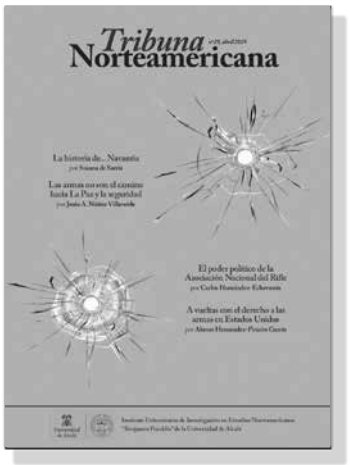
» La historia de... Gestamp. Historia de 20 años de internacionalización y crecimiento
Miguel López-Quesada
» De cómo el bilingüismo esculpe el cerebro
Albert Costa
» La controversia de la educación bilingüe en España
Víctor Pavón Vázquez
» El profesor como clave fundamental para la implementación de programas biligües de éxito
Carmen Aguilera Lucio-Villegas
» Overview of Language Development & Bilingual Education in California K-12 Schools
Karen Cadiero-Kaplan

Nº27. Julio 2018

» La historia de... Ebro en EE.U.
Antonio Hernández Callejas
» Lobbies: un acercamiento a la realidad de su influencia en la política norteamericana
Francisco Carrillo
» Los lobbies demócratas en la Era de Donald Trump
Elena Herrero-Beaumont
» El lobby americano del separatismo catalán
Francisco Javier Rupérez Rubio

Nº28. Diciembre 2018

» The United States and Spain: Using Bilateral Diplomacy to Spearhead Global Conversation Efforts
Frank Talluto
» El cambio que no cesa
Manuel Peinado Lorca
» Cambio climático y nuevo localismo. Una mirada optimista al potencial de las ciudades para contribuir a la transición ecológica de la humanidad
Bárbara Pons



Nº29. Abril 2019

» La historia de... Navantia
Susana de Sarriá
» Las armas no son el camino hacia la paz y la seguridad
Jesús A. Núñez Villaverde
» El poder político de la Asociación Nacional del Rifle
Carlos Hernández-Echevarría
» A vueltas con el derecho a las armas en Estados Unidos
Alonso Hernández-Pinzón García

Nº30. Septiembre 2019

» La historia de... Talgo en EE. UU.
Nora Friend
» I-ntentando e-xplicar lo que significa la ciberseguridad
Ángel Gómez de Ágreda
» Los claroscuros de la ciberseguridad
Yaiza Rubio
» Ciberdelincuencia en España, un desafío para el Cuerpo Nacional de Policía
Pedro Pacheco

Universidad de Alcalá

INSTITUTO FRANKLIN · UAH ·

Con la colaboración de:

FUNDACIÓN CONSEJO ESPAÑA-EE.UU.

Instituto Universitario de Investigación en Estudios Norteamericanos "Benjamin Franklin" de la Universidad de Alcalá

www.institutofranklin.net

Con la colaboracion de Iberia,
transportista aéreo preferente

IBERIA