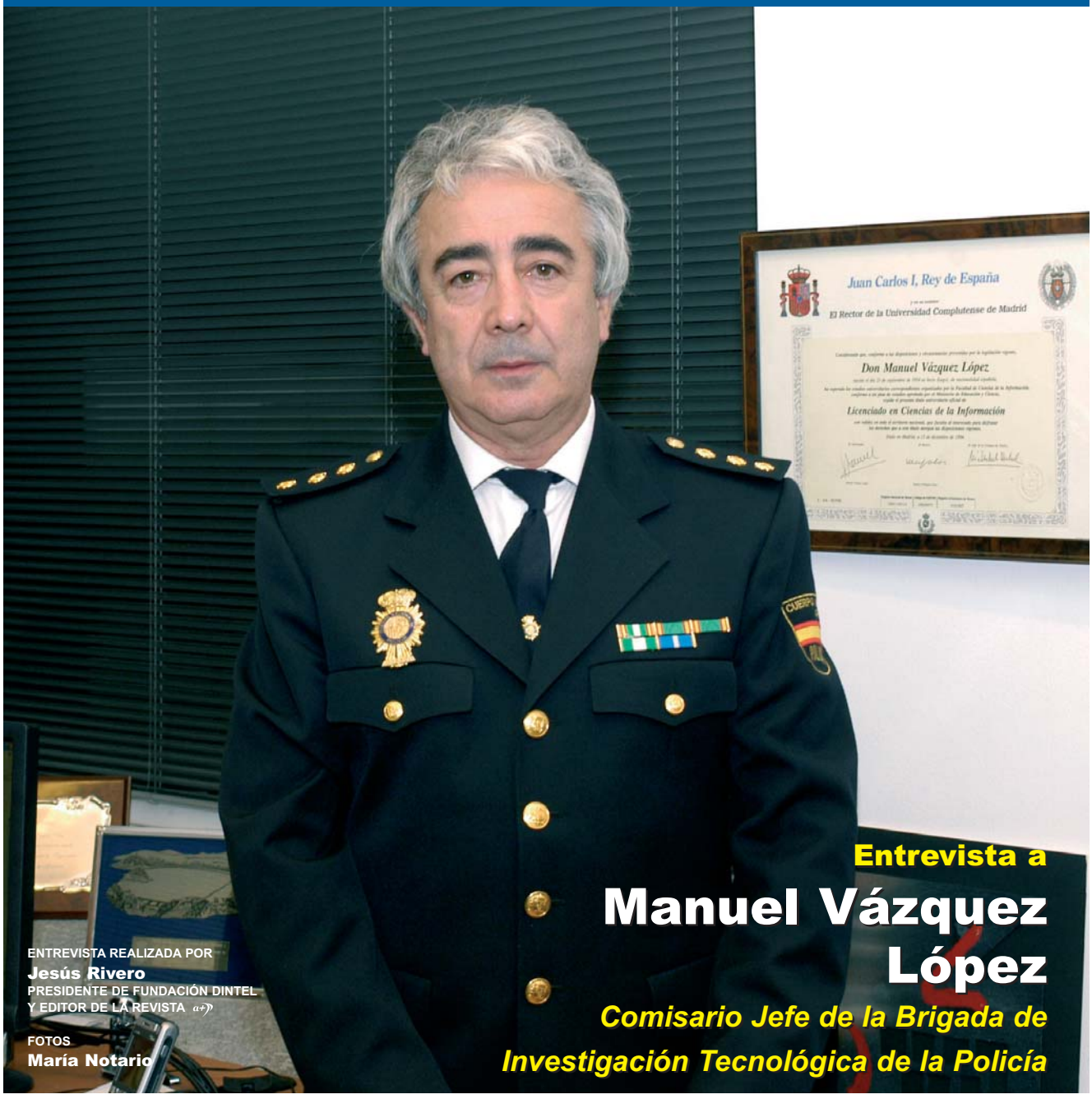
"Actualmente la Brigada de Investigación Tecnológica está en la vanguardia internacional en la lucha contra la ciberdelincuencia"



Entrevista a Manuel Vázquez López

Comisario Jefe de la Brigada de Investigación Tecnológica de la Policía

ENTREVISTA REALIZADA POR
Jesús Rivero
PRESIDENTE DE FUNDACIÓN DINTEL
Y EDITOR DE LA REVISTA a+

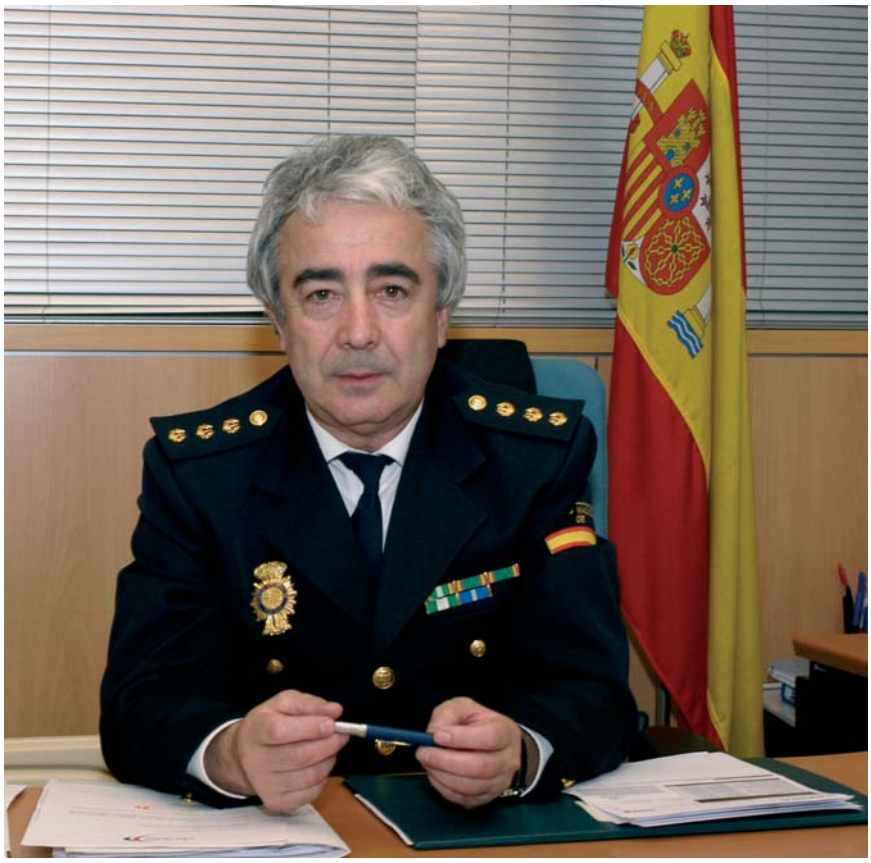
FOTOS
María Notario

Me recibe en su despacho, con "traje de calle"; y me "posa" (muy a regañadientes)... "enfundado en el uniforme": "¡soy policía!... pero mi trabajo exige discreción", me comenta.

Con el "uniforme, por dentro", el ***Comisario Vázquez López*** *es el Jefe de la Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía. Hacía tiempo que quería entrevistarle, para pedirle nos hablase –hasta donde fuese posible–, de las importantes acciones de la BIT, y de la que pasó a ser responsable cuando sustituye en el puesto al Comisario Migueláñez, en la Comisaría General de la Policía Judicial.*

No es difícil encontrar en múltiples foros técnicos al Comisario Jefe de la BIT, impartiendo conferencias y participando en debates. De verbo fluido, dinámico... siempre receptivo, quizás todo ello como consecuencia de su formación universitaria: ***Manuel Vázquez López*** *es, Licenciado en Comunicación Audiovisual por la Universidad Complutense de Madrid. También, es Máster en Dirección y Administración de la Seguridad, por la Universidad Carlos III de Madrid.*

Comisario, muchas gracias por atenderme en su despacho oficial y, concederme esta entrevista para los lectores de a+, en un número realmente especial, como éste dedicado a las TIC en la Administración General del Estado.



Antes de comenzar la entrevista propiamente dicha le agradecería nos ubique la Brigada en el ámbito global de la Dirección General de la Policía.

La Brigada de Investigación Tecnológica está encuadrada en la UDEF (Unidad de Delincuencia Económica y Financiera) dependiente de la Comisaría General de Policía Judicial que es el Órgano Directivo de la Dirección General de la Policía encargado de perseguir todo tipo de delincuencia organizada y violenta, económica y fiscal así como el tráfico de drogas y también la delincuencia tecnológica.

¿Cómo nace y por qué la BIT, o Brigada de Investigación Tecnológica de la Policía? ¿Cuáles son sus funciones y responsabilidades?

El embrión de la BIT aparece en 1995 al crearse un Grupo de Delitos Informáticos en la Brigada de Delincuencia Económica y Financiera (BDEF).

El Grupo aumenta en paralelo con la evolución de Internet y se convierte en una sección con cuatro Grupos Operativos. Finalmente en 2002 recibe el nombre actual de Brigada de Investigación Tecnológica encuadrada en la Unidad de Delincuencia Económica y Fiscal.

Para mejor ejercer sus funciones nos consta que disponen de una excelente estructura operativa en la BIT. ¿Puede detallarla para nuestros lectores?

Actualmente está estructurada en tres secciones. La primera tiene dos grupos de protección al menor encargados de investigar los delitos de pornografía infantil, teniendo como objetivo principal la detección de producción en España para rescatar a los niños que estén siendo objeto de abuso y la detención y puesta a disposición judicial de los responsables. También se realizan operaciones contra la tenencia y distribución de material pornográfico a través de los distintos canales de Internet. Otro de los cometidos importantes de estos grupos es la investigación de los casos de *grooming* y *bulling* que sean

detectados a través de las denuncias de los afectados o por cualquier otra vía.

Encuadrado en la misma sección tenemos también un grupo que investiga los fraudes en las telecomunicaciones y los delitos de calumnias, injurias, amenazas... y todos aquellos que se pueden cometer contra la intimidad de las personas, que se cometen a través de la Red.

Finalmente en esta sección se ha creado el año pasado el Grupo de Redes Abiertas, con la finalidad de navegar constantemente por la red, detectar contenidos ilícitos o delictivos e iniciar las correspondientes investigaciones si hay indicios de que puede haber materia delictiva o, en el caso de que se trate de cualquier otro tipo de infracción, ponerlo en conocimiento de las Autoridades correspondientes.

La sección segunda está formada por dos grupos que investigan los fraudes cometidos en Internet, ya sean a través de tarjetas de credito, de ventas y subastas o de medios sofisticados como es el *phishing*, *farming* o malware bancario, un grupo de seguridad Lógica para investigar aquellos delitos de carácter estrictamente informáticos como pueden ser los ataques DOS o DDOS, intrusiones, descubrimiento y revelación de secretos, etc., y finalmente un Grupo para la investigación de los delitos relativos a la propiedad intelectual e industrial.

Por último la Sección Técnica es la encargada de la formación, tanto a nivel nacional como internacional, volcados, análisis forense, I+D.

La BIT por su carácter de Unidad Central desarrolla también las investigaciones más complejas actualmente y que en el futuro, a través de los cursos que se dan a funcionarios de todas las Jefaturas Superiores, se trasmiten los conocimientos y pueden ya ser desarrolladas por otros grupos.

¿Nos puede comentar cómo son las relaciones con las policías de otros países en relación con la investigación de delitos tecnológicos? ¿Existe un grado de coordinación aceptable? ¿Qué mejoras son necesarias en este campo?

Las relaciones con las policías de otros países se realizan a través de los canales ya consolidados de cooperación policial internacional como son INTERPOL, EUROPOL, etc. Si ya en cualquier investigación policial de delincuencia organizada o tráfico de drogas la colaboración policial internacional es fundamental, en el caso de los delitos tecnológicos, por la propia arquitectura de la Red, es imprescindible. En esta línea además sería deseable que en el futuro se armonizaran legislaciones y que todos los pasos necesarios para una investigación fueran mucho más ágiles, en definitiva que las trabas burocráticas no sean un obstáculo para perseguir la delincuencia.

Actualmente la BIT está en la vanguardia internacional en la lucha contra la cberdelincuencia. Asistimos a numerosos foros internacionales que se celebran en varios países de Europa y del mundo. Sin ir más lejos este año hemos estado en Australia, Estados Unidos, Korea, en varios

países de Europa y Sudamérica y también hemos impartido cursos tanto en España como en varios países Europeos, latinoamericanos y Marruecos.

Y, con relación a la Guardia Civil, y en particular a las unidades afines: ¿existe también una adecuada coordinación de acción, en su opinión? Por el contrario, ¿existen ámbitos específicos propios en este contexto tecnológico, que les diferencien o que marquen o aconsejen actuaciones diferenciadas?

Bueno la Policía y la Guardia Civil actualmente están encuadradas en la misma Dirección General lo que necesariamente supone un elemento importante para una mejor coordinación, añadido a los órganos ya existentes como el CEMU, CICO, CNCA.

Además la Ley 2/1986 de Cuerpos y Fuerzas de Seguridad del Estado, vigente en la actualidad establece un reparto competencial que contempla dos vertientes: una la territorial que sitúa a la Guardia Civil en el territorio rural y ciudades menores de 50.000 habitantes y a la Policía en las capitales de provincia y ciudades mayores de 50.000 habitantes, y otra funcional que atribuye a la Guardia Civil competencias específicas como son tráfico, resguardo fiscal, armas, etc. y a la Policía otras como tráfico de drogas, colaborar y prestar auxilio a las policías de otros países, etc.

Naturalmente que todo es mejorable, pero respetando el marco, haciendo uso de los instrumentos de coordinación existentes y con buena voluntad por parte de todos se funciona razonablemente bien.

¿Cuáles han sido las principales actuaciones de la Brigada en los últimos tiempos? ¿Cuáles han tenido más repercusión mediática?

En el presente año se han realizado varias operaciones de gran repercusión mediática prácticamente en todos los ámbitos de la ciberdelincuencia. Sin animo de ser exhaustivo señalaría en Pornografía infantil "Carrusel" con 121 detenidos y 210 registros domiciliarios, "Lobos" con 55 detenidos e "Hydra" con 41 detenidos. En Fraudes la operación "Ulises" con 72 detenidos. En propiedad industrial "Todo en Uno" y "Buho" por venta de software ilegal y "Glamour" y "Bome" en las que se desmantelaron dos organizaciones dedicadas a la importación y venta de joyas y relojes falsos de conocidas marcas. Finalmente en Seguridad Lógica la operación "Bome" en la que se detuvo a un grupo de cinco hackers responsables de más de mil ataques a páginas entre ellas la de Izquierda Unida.

¿Nos puede facilitar algunas cifras estadísticas? ¿Qué tipos de delitos tecnológicos son más frecuentes? ¿Cómo han evolucionado estas cifras en los últimos años?

Probablemente los más frecuentes son los fraudes, así como los delitos de tenencia y distribución de pornografía infantil. En el primer caso a pesar de su frecuencia, el bajo importe unitario de los mismos hace que tengan el reproche penal no demasiado elevado, lo que supone una dificultad añadida, ya que habida cuenta la gran cantidad de pequeños delitos, hay que priorizar aquellos que sean de mayor importe o en los que concurran otras circunstancias de especial interés.

Al igual que ocurre con la duplicación o robos de tarjetas físicas, estos delitos son soportados por las entidades financieras y por los comercios virtuales, siendo en conjunto su importe muy escaso. Por ello, a pesar de un elevado número absoluto, la repercusión en los ciudadanos es escasa, ya que las

operaciones a través de Internet hoy en día ya son muy numerosas. Además, a diferencia de otros delitos contra el patrimonio "clásicos" la victimización del ciudadano es menor ya que no existe en ningún caso violencia física.

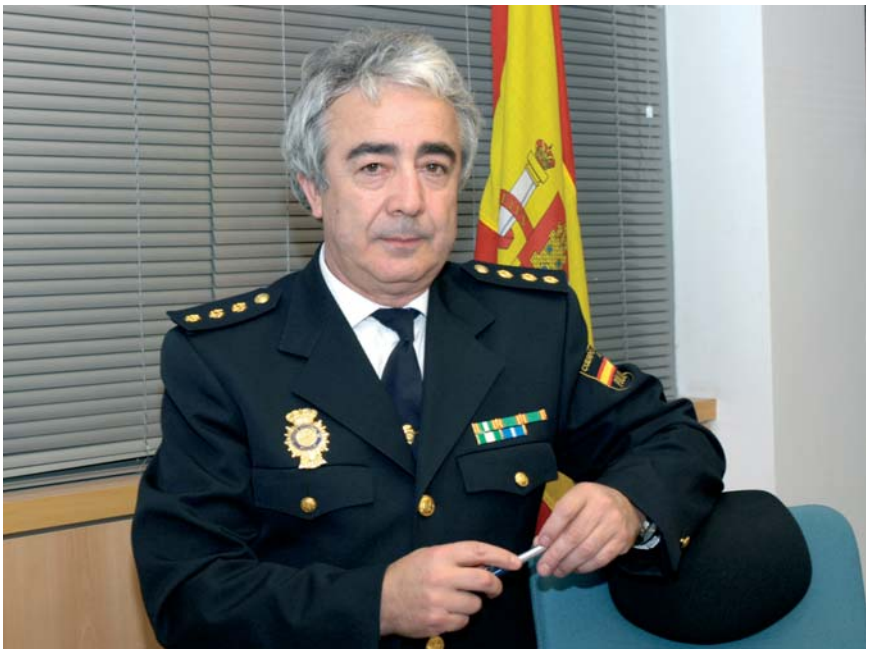
Tienen relevancia también los delitos que vulneran los derechos de propiedad intelectual e industrial y todos aquellos que se refieren a vulneraciones de la intimidad de las personas.

Por último causan mucha alarma social entre los padres aquellas conductas relacionadas con el llamado *"ciberbullying"*, esto es la utilización de las tecnologías de la sociedad de la información y de las comunicaciones, fundamentalmente la telefonía móvil y la red de Internet para acosar a un menor, conducta que le puede causar a la víctima graves problemas psicológicos, bajo rendimiento escolar, problemas de conducta, etc. Los medios más frecuentes actualmente son el uso del Messenger y las redes sociales habituales ya en institutos y colegios.

Cuando el ciber acoso tiene carácter sexual y se refiere a las acciones realizadas deliberadamente por un adulto con el fin de establecer una relación y un control emocional sobre un menor con el fin de preparar el terreno para el abuso sexual recibe el nombre de *grooming*.

Nunca son suficientes los medios humanos y tecnológicos con que se cuenta, cuando cada vez son mayores y más sofisticados los que emplean los delincuentes, pero, ¿cómo valoraría globalmente, y por ámbitos de funcionalidad, aquellos de los que actualmente dispone la Brigada? ¿Qué le pediría a sus superiores?

La lucha contra la ciberdelincuencia en general y la pornografía infantil en particular es una de las prioridades e



la Comisaría General de Policía Judicial. Los recursos humanos con los que cuenta la Brigada son muy buenos, están bien formados y, en cuanto a número, como es natural tendemos a crecer acorde con la mayor presencia no sólo ya del ciberdelito, sino que en cualquier otra actividad delictiva siempre hay material informático para analizar y estudiar.

En su opinión, ¿cuál es la mayor amenaza, con origen en los delitos tecnológicos, a la que se encuentran expuestas las empresas españolas? ¿Y los ciudadanos?

Por lo que vemos desde aquí a través de las denuncias que se interponen los fraudes perjudican gravemente a pequeñas y medianas empresas. También la vulneración de los derechos de propiedad intelectual e industrial suponen a veces una especie de competencia desleal que perjudica a las empresas que actúan bien.

No hay que descartar tampoco los casos de espionaje industrial y sobre todo que se instalara en la sociedad una desconfianza hacia la sociedad de la información y el comercio electrónico que de alguna manera ralentizara su expansión. Creo que esto sería lo más grave y debemos colaborar todos para que no ocurra.

Desde esta Brigada se mantienen contactos y relaciones con las empresas de seguridad informática privadas, siendo quizá la única asignatura pendiente la plena institucionalización de estas relaciones, como ocurre en otros países, generalmente anglosajones, donde existen, por ejemplo, instituciones en las que participan agencias policiales, otros organismos administrativos, empresas privadas, así como actores de la sociedad. Estas instituciones se encargan de temas como la prevención del fraude en Internet, o la protección de la infancia en el uso de las nuevas tecnologías, ámbitos, todos, en los que la participación de una unidad policial como la nuestra estaría sobradamente justificada.

¿Han detectado grupos organizados, dedicados a cometer delitos tecnológicos? ¿Qué nos puede comentar al respecto?

Si se han detectado Grupos Organizados sobre todo relacionados con los fraudes (*phishing*, tarjetas...) y en muy pocas ocasiones en pornografía infantil

En una operación de esta Brigada se detuvo a un grupo de más de 20 personas de una organización criminal de ciudadanos del este de Europa implicadas en un delito de *phishing* cometido desde ciber locales de España. Este delito supuso un fraude de varios millones de dólares con víctimas de Estados Unidos, Canadá, Australia y Reino Unido. Los accesos, como se ha mencionado se producían desde ciber locales españoles y en las comunicaciones utilizaban cuentas de correo anónimas.

Existía en primer lugar una gran complejidad de orden jurídico procesal (el carácter transnacional del delito, la validez de la prueba…) y por supuesto una compleja labor investigativa para demostrar los hechos y conseguir la detención de los delincuentes. Esta metodología, en la que por cuestiones obvias no se puede entrar a detallar, fueron utilizados en España por primera vez en el mundo, y se presentaron en la Conferencia Mundial de INTERPOL celebrada en el año 2005 en El Cairo. Desde entonces esta metodología se ha convertido en un estándar, no sólo para la policía española, sino también para las policías más avanzadas en la investigación de estos delitos de otros países.

Dénos algunos consejos para prevenir los delitos tecnológicos a que estamos expuestos con mayor probabilidad

En algunos delitos de los que más alarma causan como pueden ser el *ciberbullying* y el *grooming* tal como mencionamos antes, creo que los padres deben estar pendientes de lo que hacen sus hijos en la Red. Del mismo modo que nos preocupamos en qué parques están nuestros hijos, con quién juegan, cuánto tiempo están, etc., en el espacio virtual pasa un poco lo mismo y no debemos dejarlos a su libre albedrío. Mas que prohibir debemos educarlos e informarles de lo bueno que es Internet, pero que también encierra peligro. Deben saber que no pueden quedar con desconocidos, no deben acceder a fotos en la webcam para desconocidos, no dar datos de su domicilio o familia, etc.

En cuanto a las estafas acudir a sitios seguros, seguir alguna máxima ya clásica, pero perfectamente válida actualmente "nadie da duros a cuatro pesetas", acceder a banca electrónica nosotros sin contestar a ningún enlace solicitando datos, etc.

En definitiva hacer un uso responsable de Internet que es una herramienta maravillosa si la utilizamos bien.