COMPARECENCIA DEL COMANDANTE JEFE DEL GRUPO DE DELITOS TELEMÁTICOS DE LA UNIDAD CENTRAL OPERATIVA (UCO) DE LA GUARDIA CIVIL, D. ÓSCAR DE LA CRUZ YAGÜE, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 20 DE MAYO DE 2013

El señor **COMANDANTE JEFE DEL GRUPO DE DELITOS TELEMÁTICOS DE LA UNIDAD CENTRAL OPERATIVA (UCO) DE LA GUARDIA CIVIL (**D. Óscar de la Cruz Yagüe): Buenas tardes. En primer lugar, agradezco la oportunidad de estar aquí, creo que es un honor poder comparecer ante ustedes, y sobre todo en esta casa, una de las sedes en las que radica la democracia. Intentaré ser breve y conciso en varios puntos que quiero tratar, e intentar ser constructivo, es decir, aspectos que quiera poner de manifiesto de cosas que creo podemos mejorar entre todos.

En primer lugar, para ubicar dentro de la Guardia Civil cómo nos estructuramos en lo que respecta a investigaciones tecnológicas, yo represento al Grupo de Delitos Telemáticos, ya que muchas veces por tener mucha visibilidad, sobre todo en medios de comunicación, quiero decir que no somos ni mucho menos los únicos en la Guardia Civil que investigamos. Como bien decía el Director de la Guardia Civil, dentro de la estructura periférica que tiene en cada provincia, en cada Unidad nuestra que se llama Comandancia hay un grupo que se dedica a investigar todos los delitos relacionados con nuevas tecnologías en la red, que son los EDITE, y en los cuales tienen suficiente capacitación y formación como para hacer frente a todo este tipo de investigaciones.

¿Cuándo interviene el Grupo de Delitos Telemáticos? Nosotros somos una especie de segundo escalón. Cuando en estos equipos, hay investigaciones que

por necesidades de recursos humanos o materiales no son capaces de dar continuidad, o incluso hay investigaciones que afectan a varias provincias a la vez, es cuando nosotros como Unidad con demarcación nacional entramos en escena, y bien asumimos la investigación. Obviamente, también de oficio nosotros iniciamos nuestras propias investigaciones y operaciones.

Aparte de esto, existe una Unidad Técnica de Policía Judicial, en la cual no voy a incidir porque es la que representa mi compañero el Capitán Carlos Igual, pero por resumir un poco y ubicar, son los que hacen la coordinación de estas unidades periféricas así como la elaboración de inteligencia, de toda esa información que se va recopilando de la explotación de operaciones e investigaciones, ellos son los que generan esa inteligencia en cuanto a nuevos modus operandi, nuevas formas de operar que tienen los delincuentes, para luego diseminarlo otra vez a las unidades operativas.

En cuanto a las funciones del Grupo de Delitos Telemáticos, nuestro ámbito de tipología penal que perseguimos es plena; si bien hay delitos que son los más puramente tecnológicos, por así decirlo, aquellos que atacan a los sistemas de información como son las intrusiones, denegaciones de servicio, etc., hay otros tipos de delitos tradicionales que ya existían antes, pero que hacen uso de las nuevas tecnologías para su comisión. Cuando este grado de implicación de nuevas tecnologías es importante como para que haya detrás una unidad especializada en investigación de estos delitos, nosotros también asumimos su investigación.

Por esquematizar un poco estas grandes áreas, tomamos como referencia el Convenio de Ciberdelincuencia de Budapest, que se firmó en 2001, y lo categorizamos en cuatro grandes áreas. Una sería relativa a la persecución de la pornografía infantil, así como aquellos delitos que tienen como objetivo los menores (*grooming*, *cyberbullying*, abusos, acoso sexual a menores), que creo que es el área en la que más se enmarca esta ponencia. También perseguimos

todo tipo de fraudes y estafas en la red, tanto en su vertiente de comercio electrónico como bancario; perseguimos también los delitos de *hacking*, que son contra los sistemas de información, así como los delitos contra la propiedad intelectual e industrial.

También quiero hacer referencia dentro de la colaboración y cooperación, que es una de las grandes líneas que voy a tocar: en el ámbito europeo estamos en Europol y en el recientemente creado EC3, así como en grupos de trabajo de Interpol, tanto en el grupo latinoamericano como en el grupo europeo.

Y ya para entrar un poco en materia, las tres grandes líneas, por marcar primero el esquema, van a ser prevención, colaboración, y luego mejoras a nivel legislativo, que yo personalmente creo que es lo más importante y en lo que más puede mejorar nuestra calidad de trabajo y de operaciones.

En primer lugar, en cuanto a prevención, por hilar un poco actividades realizadas la semana pasada, para que vean el nivel de concienciación que tenemos nosotros con estas actividades. Aunque somos unidades operativas y nuestra función es la persecución y la investigación del delito, entendemos que gran parte del éxito es la prevención y así lo hacemos. Y aunque no sea nuestra función principal, como conocedores de esos riesgos y esas amenazas, porque es lo que estamos persiguiendo diariamente, pensamos que podemos hacer muy buena labor en este aspecto. De hecho, como comentaba, la semana pasada con ocasión del día de Internet, que fue el viernes día 17, hicimos una serie de actividades en torno a este día y a este acto. Se celebraron unas jornadas de concienciación dirigidas sobre todo a los colectivos que entendemos que tienen que tener una protección especial, como son menores, menores e incapaces (porque muchas veces aludimos solo a los menores, pero creemos que los incapaces deberían entrar bajo el mismo paraguas de protección); mayores también, de hecho uno de los talleres de formación que hicimos, de forma cariñosa se denominaba “para ciberabuelos”, porque entendemos que es gente

que está entrando en el uso y el contacto de las nuevas tecnologías y no tienen la suficiente formación como para poder detectar todas estas triquiñuelas que utilizan los delincuentes para engañarlos, lo que conocemos como ingeniería social; así como el navegante medio, ya que muchas veces no tiene los conocimientos básicos como para poder defenderse de todas estas actividades delictivas que pueden sufrir.

Otro de los actos centrales de la semana pasada fue la presentación de un libro, como ha hecho alusión el Director, escrito por un guardia civil del Grupo, que hace un año, de forma totalmente particular –aunque sabíamos de su actividad– en un blog de seguridad empezó a publicar consejos de navegación pero escritos de una forma muy sencilla, ya que al final estamos habituados a tratar en un ambiente muy técnico y hay veces que utilizamos terminología y no conseguimos llegar a quien tenemos que llegar. Él, sin embargo, utiliza un lenguaje muy básico, sin términos técnicos, para conseguir llegar a quien queríamos, al ciudadano medio, y sobre todo también a los padres, a los padres que se tienen que encargar de educar y concienciar a sus hijos. Yo me he permitido traer un ejemplar, sólo uno, porque de momento ha sido una primea edición muy limitada, y como el ejemplar se está regalando, pues no teníamos suficientes recursos como para poder traer un ejemplar para todos. De momento lo dejo aquí, pero si tienen interés en recibir algún ejemplar más, se lo haríamos llegar a posteriori.

La intención de todo esto es romper con esa brecha, esa brecha digital que es la que está haciendo que muchas veces los padres no se sientan capacitados de aconsejar a sus hijos en el uso de nuevas tecnologías. A todos nosotros de pequeños nuestros padres nos decían “no abras la puerta a extraños, no cojas caramelos de extraños en el colegio”; sin embargo, hoy en día la mayoría de los padres no saben cómo funcionan las redes sociales o las nuevas tecnologías y no tienen ese conocimiento para poder aconsejar y educar a sus hijos. En estos

talleres se ponía como ejemplo muchos padres que se encargan de llevar al niño al colegio, que no le pase nada, recogerlo, que venga acompañado y no vaya solo, y sin embargo llegan a casa y le dejan en la habitación solo con un ordenador. Entonces, es completamente ilógico. Aquí es donde sí esperamos que se pueda incidir, y sobre todo con el tema de la educación reglada en colegios.

Aunque la eficacia del plan director para la mejora de la convivencia y seguridad escolar es mucha, creemos que a día de hoy con una visita que puedan hacer una mañana, tanto Policía como Guardia Civil, en un colegio no es suficiente como para poder aleccionar a los chavales de todos los riesgos. Entendemos que ya sería momento de que en los planes de estudio se incluyera o bien una asignatura, o bien un módulo con un contenido estudiado por especialistas y que fuera adaptado a dependiendo qué rango de edad; entendemos que a menores de 8, 9 o 10 años no se les debe dar la misma formación que a adolescentes de 14 o 15, los riesgos son diferentes.

En este aspecto, quiero comentar también las labores que hacemos en cuanto a contacto con la sociedad, como son los canales de colaboración ciudadana, los cuales desde hace años intentamos potenciar porque la Guardia Civil siempre se ha caracterizado desde su servicio en el ámbito rural por estar cerca del ciudadano y hablar con la gente, que son los que al final te manifiestan sus problemas, sus inquietudes y donde se consigue mucha información para ver qué problemas están teniendo. Pues hay que trasladarlo ya al mundo digital o virtual, y por eso tanto en la página web nuestra con los canales de colaboración, aplicaciones para *smartphones*, teléfonos móviles, así como en redes sociales, lo que hacemos es poder recibir información, y a su vez es un canal de vuelta, es un canal bidireccional porque de vez en cuando lo que hacemos es publicar lo que se conoce como alertas tecnológicas para que los ciudadanos estén alerta de nuevos modus operandi, nuevas formas que tienen los delincuentes de operar.

En el ámbito de la cooperación, debido a la configuración de la red en general y de cómo operan los ciberdelincuentes, es fundamental; es un fenómeno transversal que afecta a todos los ámbitos, tanto personal como profesional, así como en la globalidad del fenómeno. Ya esos criterios territoriales con los cuales nos movíamos hasta ahora tanto en la investigación policial como judicial, es evidente que las nuevas tecnologías han acabado con ellos.

Por tanto, a nivel nacional entendemos que tanto los órganos públicos como privados que intervienen, sería aconsejable o deseable que hubiese una especie de centro nacional de coordinación, en el cual hubiera órganos tanto de cuerpos policiales, Fiscalía, Ministerio de Industria, etc. pero igual del ámbito privado, tienen que estar las operadoras, tienen que estar las redes sociales, de tal forma que esa información pueda fluir de manera sencilla y de todos para todos, no como hasta ahora, que operamos un poco en el ámbito bilateral, todos tenemos relaciones con todos, pero hacemos reuniones dos a dos, no hay ningún órgano que aglutine todos los actores y sintiendo que somos muchos los que intervenimos en aspectos de la ciberseguridad.

En el aspecto internacional, a nivel policial yo creo que tenemos canales suficientes, ágiles y buenos para la cooperación policial. En el ámbito europeo, vuelvo a incidir, está Europol con el EC3; en el ámbito internacional tenemos a Interpol. Pero sin embargo, lo que vemos es que cuando tenemos que dar el salto judicial, que suele ser casi siempre a la hora de transmitir información que tenga luego validez en un proceso penal, tenemos la limitación de que esos procedimientos no son todavía lo suficientemente ágiles como quisiéramos.

Hay una figura que es la Comisión Rogatoria Internacional por la cual, cuando necesitamos un auxilio o una información de un tercer país, ni nosotros ni el juez español lo puede pedir de forma directa; es necesario que el juez español, con esa Comisión Rogatoria Internacional, pida auxilio a un juez del

tercer país para que el juez del tercer país recopile o recabe ese auxilio o esa información y venga de vuelta a España. Estos procesos son procesos que se pueden dilatar semanas o incluso meses, por lo cual en investigaciones que, sobre todo a través de la red, son hechos que ocurren en cuestión de segundos, entendemos que no está ponderado, y muchas veces a nosotros como investigadores son situaciones que nos retrasan mucho y dificultan la investigación.

Otro aspecto, y yo creo que también es importante a la hora de solicitar colaboración internacional de algunos operadores que prestan servicios en la red, pues no todos, y sobre todo no los grandes, pero sí es cierto que hay multinacionales que, amparándose en que están sujetas a la legislación de su país, donde tiene su sede social, no colaboran todo lo bien que debieran, cuando aun así están prestando servicio a usuarios que están en España. Y ya sin entrar en temas fiscales, que creo que es otro aspecto aunque no atañe a esta ponencia, pero creo que desde España como Gobierno se debería muchas veces, si no obligar legalmente, sí exigir cierto compromiso a esas empresas que al final, son usuarios españoles que están utilizando sus servicios, y que luego cuando les vamos a requerir un auxilio policial o judicial no responden todo lo bien que debieran.

Y ya en el aspecto legislativo, que yo creo que es donde más deberíamos mejorar, porque muchas veces a nosotros nos vienen personas del entorno, de la empresa, incluso de la universidad y nos dicen “¿de qué forma os podemos ayudar para mejorar vuestra situación y vuestras investigaciones?”. Y yo siempre les digo lo mismo: más que herramientas técnicas, lo que necesitamos son herramientas legales para poder llegar más y mejor.

La ciberdelincuencia se constituye como una de las amenazas más asimétricas que hay hoy en día; es decir, los delincuentes se aprovechan de técnicas y procedimientos para delinquir que luego nosotros, como fuerzas y

cuerpos de seguridad, no podemos utilizar para investigarlos. Y aquí voy a poner dos ejemplos, uno de los cuales ya ha salido, y es la figura del agente encubierto. En el ámbito procesal actualmente se permite para investigación de terrorismo así como para investigación de determinados delitos, pero siempre en el ámbito de la delincuencia organizada. Claro, la persecución tanto de la distribución de la pornografía infantil como del acoso sexual, del *grooming* a menores no es delincuencia organizada, son individuos que de forma individual ejecutan sus acciones delictivas.

Y aquí sí que podría poner un ejemplo de la necesidad de tener esta figura para operar e investigar en Internet, y es el caso de la distribución de pornografía infantil. Actualmente la difusión de este tipo de imágenes se podría equiparar a una especie de pirámide, en la cual tenemos una base en la cual hay gran cantidad de usuarios que no toman muchas medidas de seguridad en cuanto a la difusión pero que el contenido que intercambian tampoco es de excesiva gravedad o es contenido poco actual o ya muy difundido. Esto, el ejemplo sería el ámbito de las redes *peer-to-peer*, es decir, la gente que a través de redes como Emule o Edonkey intercambian este tipo de material, pero para nosotros, como Fuerzas y Cuerpos de Seguridad, es relativamente sencillo detectarlos por unos sistemas buscadores que disponemos, en los cuales a través del material que ya conocemos, lo introducimos en el buscador, y por así decirlo de forma sencilla nos dice qué personas están compartiendo ese material.

Según vamos subiendo la pirámide, los usuarios toman más medidas de seguridad y el material es más violento, con contenido más grave, o incluso material que se produce ya por redes organizadas que mueven dinero por intercambiar este material. En estos sistemas de intercambio ya entrarían a través de correo electrónico, o incluso en foros cerrados, a los cuales para acceder es necesaria la invitación de uno de los miembros, y el contenido está cifrado. ¿Eso por qué lo hacen? Porque al pedir invitación de alguna de las

personas que ya componen ese grupo, se garantizan que nosotros no vamos a poder acceder. Hasta ahora la gran mayoría de las operaciones policiales en el entorno de la distribución de pornografía infantil se hace en las redes *peer-to-peer*, en esa base de que he hablado de la pirámide. Si incidimos solo ahí y no tocamos el techo de la pirámide corremos el riesgo de invertirla, es decir, que la gente ya sabe que gran número de operaciones policiales se hace en redes *peer-to-peer* y digan "esto no es seguro, vamos a migrar a esos foros, a los cuales es más complejo acceder". Si no implementamos figuras como la del agente encubierto, nos vamos a quedar sin herramientas como para poder acceder a esos foros y detectar qué personas están compartiendo ese material, y que normalmente es el más grave. No sé si ha quedado clara la explicación, pero luego en el turno de preguntas podemos matizarlo.

Y luego, la segunda figura que considero que es de bastante importancia para la investigación es la utilización de herramientas de administración remota de equipos. Esto es lo que popularmente se conoce como troyanos, que los delincuentes utilizan para infectar nuestros equipos y robarnos información. Actualmente nosotros no podemos utilizar estos sistemas, lógicamente sería con todas las garantías judiciales, mandamiento judicial y demás, pero actualmente no podemos utilizarlo para la investigación.

Y muchas veces, incluso yo creo que es más garante que los sistemas tradicionales, y explicaré por qué. Hasta ahora todas las intervenciones de las telecomunicaciones se hacían interviniendo el canal, es decir, todo estaba basado en la telefonía fija, con lo cual se intervenía la línea y te asegurabas de que ibas a intervenir el teléfono que el delincuente estaba utilizando. Hoy en día esto ya no sirve, ¿por qué? Porque yo con mi teléfono, con mi *smartphone* ahora me conecto por 3G, pero dentro de cinco minutos me conecto por la red WiFi de un centro comercial y a los diez minutos me voy al McDonald's y la red es diferente, con lo cual si intentamos interceptar el canal no vamos a conseguir

nada porque el canal va cambiando. Por eso entendemos que es muchísimo más efectivo a día de hoy intervenir el dispositivo; independientemente del canal que me conecte, yo voy a tener garantizadas las comunicaciones de ese terminal. ¿Por qué digo también que es más garantista? Porque interviniendo el canal, cualquier persona que utilizara ese teléfono fijo de la familia, van a quedar registradas sus conversaciones. Sin embargo, intervenir un teléfono móvil, normalmente a día de hoy es personal y lo utiliza una sola persona.

Otro aspecto del que quería hablar, y ya lo ha comentado el Director, es el tema de lo sencillo que resulta a día de hoy conseguir anonimato en la red, empezando por lugares públicos, como son locutorios, cibercafés, universidades, colegios, etc. No se puede tener un control total sobre qué personas utilizan cada servicio, pero sí que a lo mejor sería deseable llevar una especie de control administrativo sobre las personas que utilizan un determinado servicio de Internet en los locutorios, por ejemplo, en Internet. De hecho, hace algunos años tuvimos que sufrir las consecuencias de un atentado como fue el 11-M para darnos cuenta de que el que hubiera tarjetas de teléfono prepago anónimas era un grave problema de seguridad. Pues bien, a día de hoy los mismos efectos que se pueden generar con un teléfono móvil por GSM de activar un explosivo o una bomba remota, se puede conseguir igualmente con el mismo teléfono conectado a una red WiFi y de forma totalmente anónima. Entendemos que es una brecha bastante grave de seguridad y que nunca se tiene que confundir con el contenido. Lo que entendemos que hay que controlar es qué persona realiza la conexión en cada momento, independientemente luego del contenido material, que eso en ningún momento se ve afectado, de la comunicación.

Quiero reiterar también, en cuanto a aspectos de legislación, que ya se ha hablado, en materia penal, intentar adaptar a las nuevas realidades los tipos penales, que hasta ahora lo que se iba haciendo era adaptar tipos que ya existían, intentar encajarlos en los nuevos delitos como se cometen en la red. No siempre

es efectivo, y entiendo que eso, tanto a las Fuerzas y Cuerpos de Seguridad como incluso las víctimas les genera inseguridad; inseguridad jurídica de ver que los tipos tal y como se están cometiendo a través de las nuevas tecnologías no es equiparable al delito como está tipificado en el Código Penal.

Y ya por acabar, también quería comentar que, a lo mejor, puesto que tenemos un sistema judicial yo creo que un poco saturado, debido a que hay demasiadas conductas que están tipificadas como delito o como falta, pues a lo mejor sería conveniente potenciar el derecho administrativo para las circunstancias menos lesivas o menos graves; quizá, una suplantación de identidad simplemente, sin que vaya acompañada de nada más, que no haya injurias o amenazas, a lo mejor sería más sencillo de resolver simplemente con un procedimiento administrativo, al modelo de como se hace con la protección de datos de carácter personal, que al final para nosotros es casi más efectivo, porque las garantías procesales no son las mismas que en un proceso penal, y la sanción social que recibe es una multa económica, y muchas veces creemos que es casi más efectivo que no un proceso penal que se dilata en el tiempo, y luego la respuesta que se le da a ese delito no está equiparada con la sanción que lleva asociada.

Por mi parte nada más; muchas gracias por su atención, y a su disposición para las preguntas.