Ciberriesgos, procedencia y dificultades en la investigación policial

José Durán Martín // Teniente coronel de la Guardia Civil

La Guardia Civil en el ciberespacio

La Guardia Civil, junto al resto de fuerzas y cuerpos de seguridad, tiene la misión de proteger el libre ejercicio de nuestros derechos y garantizar la seguridad ciudadana. Y, aunque con distintas formulaciones, ha estado llevando a cabo esta misión desde los tiempos de su fundación en 1844. Al principio únicamente por tierra, pero a medida que la Institución fue creciendo en entidad, funciones y competencias, se vio avocada a hacer uso también del medio aéreo y marítimo. Y, como no podía ser de otra manera, a mediados de la década de los 90, la Guardia Civil creó el entonces llamado Grupo de Delitos Informáticos para atender a la todavía incipiente demanda de los ciudadanos.

> La Guardia Civil también ha evolucionado, creciendo y adaptándose a las nuevas circunstancias, lo que le ha llevado a dotarse con Unidades muy especializadas dedicadas a amenazas como el hacktivismo o ciberterrorismo

Casi un cuarto de siglo después, Internet ha sufrido una tremenda transformación, y con ella, ha transformado las comunicaciones, los negocios, las relaciones personales, el ocio, en definitiva, el mundo. Y lo ha hecho hasta el punto de que podemos afirmar que se ha creado una nueva dimensión de la realidad, una dimensión en la que vivimos gran parte de nuestras vidas, que denominamos ciberespacio y que, como explicaremos más adelante, no está en absoluto exenta de amenazas y riesgos para ciudadanos, empresas e instituciones.

La Guardia Civil también ha evolucionado, creciendo y adaptándose a las nuevas circunstancias, lo que le ha llevado a dotarse con Unidades muy especializadas dedicadas a amenazas como el **hacktivismo** o **ciberterrorismo**. Además, en el ámbito de la lucha contra la **ciberdelincuencia**, la pequeña unidad creada en 1996 se ha convertido en una de las unidades más reconocibles y mediáticas de la Guardia Civil, el **Departamento de Delitos Telemáticos** de la Unidad Central Operativa. Además, contamos con un **Grupo de Delitos Tecnológicos** dentro de la Unidad Técnica de Policía Judicial, nuestra Unidad de Inteligencia Criminal, y con un importante y avanzado **Laboratorio de Informática Forense** encuadrado en el Servicio de Criminalística de la Guardia Civil. Adicionalmente, contamos con especialistas en investigación tecnológica desplegados por todo el territorio nacional, los denominados EDITEs, que suponen un primer escalón de proximidad para el ciudadano.

Al margen de estas capacidades, todas dedicadas a la lucha contra el cibercrimen, la Guardia Civil también se ha visto en la necesidad de proteger sus sistemas e infraestructuras informáticas. Recordemos que la Guardia Civil es una institución que cuenta con unos 80.000 efectivos y más de 2.000 instalaciones desplegadas por todo el territorio nacional. Esto supone una tremenda superficie de exposición que, unido al hecho de que la información que se gestiona, sobre terrorismo, crimen organizado, sobre nuestros ciudadanos… es ciertamente muy sensible, hace que la securización de los sistemas utilizados sea de vital importancia. En este aspecto, la unidad competente es la **Jefatura de Servicios Técnicos**.

El último actor, dentro de la Guardia Civil, en incorporarse a todo este abanico de recursos dedicados de una manera u otra a la ciberseguridad ha sido la **Unidad de Coordinación de Ciberseguridad**. Creada formalmente en 2019 y puesta en marcha a principios del 2020, tiene entre sus funciones las de servir de Punto de Contacto institucional de la Guardia Civil para la interlocución en materia de ciberseguridad, así como la definición de criterios de coordinación y optimización del potencial disponible para hacer frente a las ciberamenazas, impulsando la actuación coordinada de las distintas unidades con competencias en ciberseguridad.

Obviamente, existe una demanda creciente en la ciudadanía, empresas e instituciones que empujado a

la Guardia Civil a crecer en capacidades. Sin embargo, es preciso señalar también la existencia de referencias a nivel estratégico, como la Estrategia de Seguridad Nacional (2017) y, sobre todo, la **Estrategia Nacional de Ciberseguridad de 2019** y el Plan Estratégico contra la Cibercriminalidad del Ministerio del Interior aprobado durante el presente mes de marzo. Todas estas directrices estratégicas, impulsan a la Institución a luchar contra todas las formas de criminalidad en Internet manteniendo actualizadas sus capacidades y adaptándose a la evolución de las distintas amenazas. También suponen que la Guardia Civil contribuya a la difusión de la Cultura de ciberseguridad, cuestión que sin duda se lleva haciendo muchos años y en diversos frentes, pero que ahora se pretende relanzar desde la **Unidad de Coordinación de Ciberseguridad** mediante el establecimiento de un plan concreto a tal efecto.

Ciberamenazas

Volviendo a los riesgos existentes en el ciberespacio, y entendiendo estos como la probabilidad materialización de una determinada ciberamenaza, causando pérdidas o daños, mencionaremos a continuación algunas de las ciberamenazas que más preocupan a las agencias policiales de todo el mundo.

En primer lugar, tenemos el fenómeno del **ransomware**, que hace años que se mantiene como la amenaza más prevalente y dañina desde el punto de vista económico. Como aspecto novedoso se puede indicar que se observa cómo los ataques ya no son totalmente indiscriminados, sino que se realizan de manera cada vez más dirigida a empresas y entidades, tanto del sector público como privado.

Otro de los ciberataques que más pérdidas está produciendo a las empresas es el denominado **BEC *(Business Email Compromise)*** que, aunque puede tomar muy diversas formas, básicamente consiste en engañar a un empleado para que realice un pago de una factura falsa a una cuenta bancaria controlada por los cibercriminales. En ocasiones se trata de simples engaños, "ingeniería social" sencilla que, por un motivo u otro, llega a funcionar. Pero también podemos encontrar ataques muy sofisticados desde el punto de vista técnico y que implican intrusiones en los sistemas de la empresa atacada o sus proveedores.

Las **fugas de información** son otro de los incidentes de ciberseguridad más frecuentes. Aquí la casuística es también muy variada y encontramos desde ataques relativamente sencillos hasta otros llevados a cabo por grupos vinculados a actores estatales. Lo que sí podemos afirmar es cualquier tipo de información puede ser de interés. No pensemos que los cibercriminales únicamente buscan credenciales de acceso a banca *online*, o datos de medios de pago. Muy al contrario, los criminales tratan de sacar partido a todo tipo de información, y otros datos personales, que pueden no ser directamente *"monetizables"*, pueden llegar a tener un valor potencial incluso mayor al permitirles extorsionar a empresas, o realizar gracias a esa información ataques más complejos como los BEC antes mencionados. Otro aspecto a valorar con respecto a este tipo de ataques son las consecuencias legales e importantes multas que pueden imponerse en determinadas circunstancias.

Otro aspecto que lleva años cobrando relevancia creciente son los **ataques a la cadena de suministro** que, precisamente son el origen de muchas de las fugas de información de las que acabamos de hablar. Y es que se observa una tendencia creciente en el uso de clientes, proveedores y *partners* como una forma de atacar un objetivo que, a priori, puede estar mejor protegido. Todos los negocios forman parte de una cadena y, aunque resulte obvia la afirmación, esta es tan fuerte como el más débil de sus eslabones.

Por último, y, aunque no se trata de un ciberataque propiamente dicho, los ataques de **desinformación** o ***fake news*** sí que pueden llegar a ser una amenaza para nuestras empresas y, obviamente, se trata de una amenaza que se propaga por el ciberespacio. La solución en estos casos pasa por la concienciación, prevención, y gestión de la comunicación, más que por medidas de ciberseguridad propiamente dichas.

Retos para las investigaciones policiales

¿Qué podemos hacer al respecto de todas estas amenazas? Pues desde el punto de vista policial la respuesta es obvia: investigar, como con cualquier otro delito. Sin embargo, las investigaciones tecnológicas tienen una serie de dificultades añadidas o peculiaridades que precisamente derivan de la propia naturaleza de las conductas que se investigan. Aunque el objetivo de una investigación policial es siempre el mismo (identificar autor de un delito y obtener pruebas de su comisión), las investigaciones tecnológicas normalmente van a afectar a procesos de comunicación, que están especialmente protegidos en la mayoría de los ordenamientos jurídicos y, desde luego, en el nuestro. Además, las técnicas de investigación tradicionales resultan insuficientes, siendo necesario utilizar y aprovechar la potencialidad de las herramientas tecnológicas que,

Foto: iStock.com/peshkov

además, van a tener que ser utilizadas por personal altamente especializado. Estos factores van a condicionar y, en cierto sentido, a dificultar las investigaciones.

Por un lado, nos vamos a encontrar una serie de **dificultades relacionadas con la imposibilidad por parte de los investigadores de acceder a información necesaria** para la investigación.

- En primer lugar, tenemos los **proveedores de servicios de comunicaciones vía IP**, que actúan con independencia de la red de telecomunicaciones que les da soporte. Servicios como WhatsApp, Telegram, etc. son usados para mensajería, llamadas de voz, videollamadas, etc. Estos servicios, no están normalmente sujetos a la normativa de interceptación de comunicaciones, ni tampoco a la de Conservación de Datos, con lo que el acceso a dichas comunicaciones resulta muy complejo para los investigadores.
- Precisamente, las **diferencias entre los distintos regímenes de Conservación de datos** y, en ocasiones, la inexistencia de estos, también supone un gran reto para los investigadores. Sin embargo, este tipo de información que, recordemos, no incluye el contenido de la comunicación sino sólo datos asociados a dicha comunicación, ha demostrado ser útil en casos tan complejos como el caso de Diana Quer.
- La creciente implementación de **tecnologías de cifrado por defecto** en todo tipo de dispositivos y comunicaciones supone también un hándicap. Aunque el cifrado tiene un evidente efecto positivo en el ámbito de la ciberseguridad, es también innegable que dificulta extremadamente algunas técnicas de investigación como la interceptación de comunicaciones o el análisis forense de dispositivos electrónicos, fundamentales para la investigación criminal.
- También el uso de **criptomonedas** y otros servicios asociados que incrementan el anonimato y actúan a modo de cortafuegos, impiden a los investigadores seguir el flujo del dinero, y complican significativamente la recuperación de activos y las actividades de prevención de blanqueo de capitales y de transacciones fraudulentas.
- Por último, también en este grupo de dificultadas relacionadas con la incapacidad de los investigadores de tener acceso a información relevante para sus investigaciones, quiero mencionar la elevada **"cifra negra"** existente. Es decir, delitos que no son denunciados y que, por tanto, no existen a efectos de investigación policial. Es necesario realizar, y se está haciendo

desde Guardia Civil, una labor de concienciación en este sentido, ya que cuanta más información tengamos, mayores serán las posibilidades de éxito de la investigación.

También nos encontramos toda una serie de **problemas relacionados con la determinación de una ubicación de interés para la investigación**, ya sea la ubicación física del ciberdelincuente, de la infraestructura tecnológica usada en la actividad criminal, de las pruebas electrónicas, e incluso en ocasiones, como en el caso de algunos delitos sexuales contra menores, de las víctimas. En estas situaciones normalmente no está claro qué país tiene jurisdicción para investigar, obtener evidencias ni perseguir judicialmente a los cibercriminales, lo cuál puede suponer un grave perjuicio para la investigación.

- Así, por ejemplo, nos encontramos que existen tecnologías como *blockchain*, usada en el ámbito de las **criptomonedas**, que están basadas en sistemas distribuidos, y que carecen de autoridad central a la que dirigirnos para, por ejemplo, bloquear una determinada cuenta o transacción y/o solicitar información sobre los intervinientes.
- Por otro las **tecnologías de anonimización** como VPNs, y Darknets como Tor, I2P, etc. que ofrecen anonimato a sus usuarios, e imposibilitan o dificultan la determinación de la ubicación física de la máquina que están usando, permiten la proliferación de mercados y servicios criminales.
- Incluso el, hoy generalizado, uso de **servicios y almacenamiento en la nube**, que hace que la información pueda encontrarse simultáneamente, o de forma fragmentada, en diferentes jurisdicciones, también plantea problemas a la hora de determinar qué jurisdicción es la competente para acceder a datos relevantes para las investigaciones.

Finalmente es necesario recordar que la mayoría de las investigaciones tecnológicas cruzan las fronteras de un país y hacen necesaria la utilización de mecanismos de cooperación internacional que se ven dificultados por las **diferencias entre los distintos marcos normativos nacionales**.

- Estas diferencias, que suelen responder a una **transposición incompleta de instrumentos de cooperación internacional**, se dan principalmente en cuanto a: conductas criminalizadas en sus respectivos códigos penales y/o medidas de investigación previstas en sus leyes procesales.
- Tampoco existe en la actualidad un marco que permita el intercambio o **remisión rápida de evidencias digitales**, como si ocurre con la preservación rápida (arts. 16 y 17 Convenio Budapest). En la práctica, los tiempos de los procedimientos de Asistencia Jurídica Mutua en materia penal pueden llegar a poner en peligro la eficacia de las investigaciones.
- Resulta igualmente necesario reconocer que nos resulta **imposible legislar al ritmo que marcan los avances en tecnología** y el uso criminal de éstos. La justicia siempre ha corrido detrás de los delincuentes, pero en la actualidad se podría afirmar que la distancia entre unos y otros va en aumento y resulta difícil de reducir.
- Finalmente, otra deficiencia comúnmente observada en muchos países es la **falta de regulación específica sobre las investigaciones *online*** que, sin duda, dificulta la colaboración policial internacional y pone en peligro el buen fin de las investigaciones.

> La mayoría de las investigaciones tecnológicas cruzan las fronteras de un país y hacen necesaria la utilización de mecanismos de cooperación internacional que se ven dificultados por las diferencias entre los distintos marcos normativos nacionales

Por fortuna podemos decir que, desde 2015, España cuenta con una moderna regulación que, al menos en parte, nos ofrece los instrumentos jurídicos necesarios para enfrentarnos a muchos de los retos y problemas mencionados. Así, la Ley orgánica 13/2015 viene a regular aspectos tales como la figura del agente encubierto *online*, el registro de dispositivos electrónicos y su posible extensión a terceros sistemas legalmente accesibles desde el dispositivo registrado, el registro remoto de dispositivos… y muchas otras medidas de investigación tecnológica que, ofreciendo los máximos estándares en cuanto a garantías para los ciudadanos, ofrecen soluciones legales para que los investigadores puedan hacer su trabajo. ●