La Guardia Civil advierte de que el ciberdelito está creciendo anualmente a un ritmo de hasta el 50%

El coronel y director de la División de Tecnología de este cuerpo, Luis Fernando Hernández, ha dicho que las cifras del daño causado a nivel mundial ya son «multimillonarias»

El coronel y director de la División de Tecnología de la Guardia Civil, Luis Fernando Hernández, ha impartido hoy una ponencia sobre los **múltiples peligros cibernéticos** que existen en la sociedad y, por ende, en la estructura financiera, económica y productiva del país, con especial énfasis en **el ciberdelito que, según ha explicado, está creciendo anualmente a un ritmo entre el 40% y el 50%** con respecto al año anterior. Así lo ha señalado en una de las conferencias programadas dentro del curso de verano «Finanzas sostenibles y su importancia en el futuro de la economía», organizado en Santander por la Asociación de Periodistas de Información Económica (APIE) y la Universidad Internacional Menéndez Pelayo (UIMP).

El experto ha definido, al comienzo de su intervención, el concepto de ciberamenazas como un «conjunto difuso de elementos hostiles que operan en el ciberespacio y que tienen unas finalidades muy concretas» y ha mencionado, **por orden de gravedad, cinco grandes bloques en cuanto a la motivación: ciberespionaje, ciberdelito, hacktivismo, ciberterrorismo y ciberguerra.**

Del **ciberespionaje** ha dicho que hay de carácter político, militar y también económico y que «su objetivo fundamental suelen ser las instituciones públicas, pero también los intereses económicos de valor estratégico». Hernández ha señalado que, cuando se reflexiona sobre los agentes, «estamos acostumbrados a que se nos hable de los ejes del mal, de China, Rusia, Irán o Corea del Norte. No quiere decir que no sean unos vectores de amenaza muy a tener en cuenta, pero también hay otros agentes muy próximos a nosotros, que incluso consideramos aliados. En realidad en el campo de la guerra económica no hay amigos ni aliados, solo competidores». El experto ha añadido que **al enemigo no hay que buscarle en la otra punta del mundo**. Piensen en cualquier sector productivo y cuál es su directo competidor: ahí tienen al enemigo, al potencial vector de ataque. Esa es la cruda realidad».

«Hay muchas personas que han sido objeto de ciberdelito, sobre todo los más jóvenes, que son hiperactivos en redes sociales y otras plataformas»

En segundo lugar, el coronel de la Guardia Civil ha abordado el **ciberdelito**, del que ha resaltado que está experimentando un crecimiento «ya no exponencial, sino viral». En este sentido, ha destacado que está creciendo anualmente a un ritmo entre el 40% y el 50% con respecto al año anterior. **«las cifras del daño causado a nivel mundial ya son multimillonarias y, a nivel nacional, son muy considerables**», ha indicado el experto en ciberseguridad, que ha apuntado que, además, el ciberdelito tiene un factor muy desestabilizador, que es la alarma social que está generando. Según sus palabras, «hay muchas personas que han sido objeto de ciberdelito, sobre todo los más jóvenes que son hiperactivos en redes sociales y en otras plataformas».

El director de la División Tecnológica de la Guardia Civil ha asegurado que los ciberdelincuentes buscan monetización y que, por consiguiente, los objetivos son todos aquellos que les puedan aportar beneficio económico. Sin embargo, ha precisado que «**en este momento lo que más interés tiene en la red oscura es la compraventa de datos de empresas y datos personales**». Acerca de quiénes están detrás de este tipo de operaciones, ha apuntado a las organizaciones criminales, pero también terroristas: «Existe constancia de que en su momento Al Qaeda lo hizo y en este momento Daesh también. Están utilizando el ciberdelito para financiar sus actividades». En este contexto también se ha referido a los servicios de inteligencia, que pueden recurrir al ciberdelito debido a que es «una forma de desestabilización y de subversión».

A continuación, Hernández se ha centrado en el **hacktivismo**. Ha aclarado que en España es de muy baja intensidad, aunque a nivel global hay mucha actividad. El experto ha dicho que, dentro del hacktivismo, son muy típicas las que se denominan **acciones de falsa bandera**, es decir, los hechos que se producen y que tienen una atribución cuando en realidad han sido provocados por otros.

En lo relativo al **ciberterrorismo**, ha matizado que hay dos acepciones del concepto: por un lado, el uso de Internet y de las tecnologías en beneficio de la acción terrorista, que es lo habitual, y, por otro lado, Internet y las tecnologías de la información como objetivo de la acción terrorista.

El experto ha resaltado que «el ciberterrorismo está considerado una **amenaza emergente de baja probabilidad pero alto impacto**, lo que quiere decir que la probabilidad de que mañana se produzca una acción ciberterrorista es escasa, pero si se produjera el impacto sería brutal. No lo dice solo la Guardia Civil, también la Comisión Europea». De la ciberguerra no ha querido profundizar ya que, como ha dicho, se enmarca en el ámbito de las fuerzas armadas.

«El ciberterrorismo está considerado una amenaza emergente de baja probabilidad pero alto impacto»

El director de la División de Tecnología de la Guardia Civil ha destacado que, como reconoce la Unión Europea, **España es uno de los países más avanzados dentro de la Unión en ciberseguridad desde el punto de vista formal y regulatorio**. Sin embargo, ha lamentado que en nuestro país «no hay asignación económica ni presupuestos asociados» y ha recordado que «la única forma de que el estado protegiera a las empresas es que operase sus sistemas informáticos, lo que escandalizaría a todos. La ciberseguridad depende de las propias empresas y el nivel de inversión en España es muy bajo».

Sobre las posibles causas de la baja inversión por parte de las organizaciones en ciberseguridad ha apuntado que **el retorno de esa inversión no es tangible**, «lo que hace que la mayoría de las veces se produzcan los recortes en ciberseguridad. Eso solo se puede combatir a base de concienciación».

Acerca del veto de Donald Trump a Huawei , Luis Fernando Hernández se ha mostrado contundente: «**Huawei lleva presente en España 14 años, todas las plataformas 4G y 3G de la principal operadora del país son de esta compañía y no pasa nada**». De esta forma, el experto en ciberseguridad ha aludido a que la multinacional china tiene la mitad de las patentes mundiales de 5G, cerca de 3.000 que, si se unen a ZTE y alguna otra empresa del país, se obtiene que tres cuartas partes del estándar 5G está en manos de empresas chinas, mientras que las americanas tienen 200 patentes.

El problema de fondo, ha dicho, es que «en este momento la tecnología de las empresas chinas está tres o cinco años por delante de la de las empresas americanas, es una guerra comercial». «**Estados Unidos no ha presentado ninguna prueba**, hasta ahora solo hay titulares. Lo que sí es un hecho es que Estados Unidos tiene abierta una guerra comercial con el resto del mundo», ha concluido.

Fuente: ABC