Las amenazas de nueva generación para las empresas

Félix Arteaga | Investigador principal de Seguridad y Defensa, Real Instituto Elcano

Cuando todavía no se ha conseguido concienciar a todas las empresas e industrias de los riesgos de ciberseguridad a los que se enfrentan, aparecen en el horizonte nuevos riesgos de la mano de la hibridación y la digitalización que pueden poner en peligro el tejido empresarial y la continuidad de algunos negocios. En consecuencia, y como señala un reciente Informe de Panda Security, las empresas deben afrontar una "revisión profunda" de su gestión de ciberseguridad si desean preservar un nivel aceptable de ciber-resiliencia.

"(...) las empresas deben afrontar una "revisión profunda" de su gestión de ciberseguridad si desean preservar un nivel aceptable de ciber-resiliencia".

Carlos Galán analiza exhaustivamente las **amenazas híbridas** en un documento de trabajo, por lo que sólo queda en este comentario aprovechar su aparición para avisar a los cibernavegantes de la tormenta que se avecina. Por un lado, la competencia geoeconómica de las grandes potencias está detrás de gran parte de los ciberataques sobre el sector industrial y empresarial dentro de lo que podría denominarse una "guerra económica de amplio espectro" (*Broad Economic Warfare*, siguiendo a Shmuel Even, del INSS de Tel Aviv). Tras la introducción de las ciberherramientas en esa competición económica global, se añade ahora la carrera por alcanzar tecnologías disruptivas como la inteligencia artificial, la automatización, la robotización o la computación cuántica, entre muchas otras. Empresas y Estados buscan liderar la disrupción tecnológica para alcanzar antes que los demás unas posiciones de preeminencia —si no de hegemonía— económica mundial. Llegar antes que los demás les otorgará una ventaja comparativa sin precedentes en sus aplicaciones a la economía, la industria, la política y otras, desalojando a sus competidores de las posiciones de privilegio que les otorgó la Revolución Industrial. Los primeros en llegar se quedan, prácticamente, con todo y los que llegan después deben competir por las migajas (nichos) menos lucrativos del mercado.

Las empresas españolas —y las europeas— ya conocen de primera mano el coste de la **dependencia tecnológica** en materia de ciberseguridad, el precio a pagar y los riesgos asociados a los monopolios. Por eso la Comisión Europea plantea la batalla de la soberanía tecnológica, para mitigar y, en lo posible, revertir la ciberdependencia respecto de las grandes potencias industriales y estatales. Yendo por detrás, la batalla de la UE no se puede plantear sólo en términos reactivos, limitándose a prevenir los ataques, sino también en términos anticipatorios; es necesario invertir en resiliencia, pero también en anticipación.

Otro campo de batalla que la Comisión está abriendo es el del cribado de las inversiones directas de terceros países en sectores estratégicos para la ciberseguridad de la UE y

del que da idea el estudio de Copenhagen Economics. Pretende emular a Estados Unidos, Australia o Japón y evitar la adquisición de activos estratégicos para la tecnología europea frenando la compra de conocimiento, talento y capacidades industriales por parte de países como China. La batalla se también se da por el liderazgo de la próxima generación de redes 5G, según describe el estudio de Eurasia Group "The Geopolitics of 5G", y explica las medidas contra firmas chinas como Huawei y ZTE que aparecen últimamente en titulares como los que recoge el número de diciembre de CIBER elcano.

Más allá de la competición geoeconómica entre los grandes, las empresas tendrán que afrontar a medio plazo el mismo tipo de competencia desleal entre iguales, nacionales o extranjeros, porque más pronto que tarde acabarán utilizando las mismas herramientas que los anteriores. La hiperconectividad pone al alcance de las empresas instrumentos de competición que, por ahora, están desarrollando y probando las grandes empresas y Estados, pero ese *know-how* se acabará trasladando inevitablemente desde el lado oscuro de los gobiernos al lado oscuro de las consultoras y a los responsables de *marketing* menos éticos. Así como ha ido creciendo como servicio la contratación de ciberdelincuentes, no tardará en ofrecerse la desinformación como servicio para competir deslealmente u otros instrumentos probados *en combate* por las grandes potencias nacionales y empresariales.

Para las empresas, las amenazas no son la globalización, la digitalización o la revolución industrial en todas sus manifestaciones, sino los actores que se aprovechan de los instrumentos desleales que las anteriores permiten para competir deslealmente. La *hibridación* de las amenazas, es decir, la proliferación y combinación de agentes, modos y objetivos, cambia las reglas del libre mercado. En la figura 1, se muestra la progresiva hibridación de la competición económica, desde los modos y agentes que utilizaron el ciberespacio para poner en riesgo la seguridad nacional a su combinación con fuerzas y actuaciones militares en la llamada "guerra híbrida", de la que se ocupa la defensa nacional, hasta, finalmente, su utilización para deteriorar la prosperidad económica de los Estados y sociedades.

"La hibridación de las amenazas, es decir, la proliferación y combinación de agentes, modos y objetivos, cambia las reglas del libre mercado".

Figura 1. La *hibridación* de la competición económica

Tipos	Agentes	Modos (ciber)	Objetivo
ciberseguridad	estados individuos	ciberataques disrupción revelación espionaje	seguridad nacional
guerra híbrida	**los anteriores** **+ fuerzas armadas** **+ paramilitares** **+ insurgencia**	**los anteriores** **+ agresión armada** **+ guerra información** **+ subversión**	**defensa nacional**
amenazas híbridas	los anteriores + grupos + activistas + facilitadores + redes	los anteriores + influencia + sabotaje + desconfianza	seguridad económica

Como se refleja en la figura anterior, las empresas que no prestan servicios ni infraestructuras críticas no tienen que preocuparse apenas por las amenazas a la seguridad nacional y a la defensa nacional. Los agentes y modos de agresión no se dirigen directamente contra ellas, sino contra los Estados, su funcionamiento y reputación, lo que explica la implantación y el desarrollo de la ciberseguridad nacional. Sin embargo, el proceso de hibridación, es decir, la proliferación de nuevos actores y modos como los que se reflejan en la figura, sí que les afecta en la medida en que su objetivo afecta ahora a la seguridad económica. La hibridación permite la cooperación entre agentes viejos conocidos de la ciberseguridad: Estados y *hackers* con grupos criminales, comerciales, activistas, facilitadores y redes de comunicación a su servicio que cooperan entre sí para obtener ganancias económicas o alterar la libre competencia. Además, intercambian modos de actuación y herramientas desarrollados por los Estados para la competencia global y los transforman en nuevas fuentes de inseguridad económica.

Como resultado, las empresas e industrias se enfrentan a un mercado que se va llenando de nubarrones en forma de competencia geoeconómica, proliferación de ciberataques, falta de regulación, desinformación y disrupción tecnológica. La hibridación afecta a todas las facetas físicas, reputacional, de la información, de los sistemas y digital. Para prevenir o mitigar los efectos de la hibridación, la respuesta debe ser también híbrida, para lo que hace falta articular una combinación de actores (públicos y privados) y medios (defensivos y ofensivos). La coordinación actual es limitada y está enfocada a las prioridades de seguridad nacional, las infraestructuras críticas, la Administración y los sectores estratégicos, pero no basta para cubrir la seguridad económica del tejido empresarial y económico. Para afrontar la tormenta que se avecina, los anteriores necesitan integrar (hibridar) sus distintas capacidades de seguridad y combinarlas con las del sector público, incorporar nuevos instrumentos y cambiar el modelo de gobernanza. La próxima revisión de la Estrategia de Ciberseguridad Nacional presenta una buena ocasión para avanzar en la

contrahibridación; de lo contrario, las empresas e industrias se dirigen sin remedio contra una tormenta perfecta.