CIBERSEGURIDAD: LA INMENSA FRAGILIDAD DE LA RED 5G

Por: Miguel Ángel García Vega. Ethic. 26/09/2019

La red inalámbrica promete la conectividad total pero es muy susceptible a los ciberataques y sus consecuencias podrían ser catastróficas. ¿Hemos abierto la puerta a una Arcadia digital para los 'hackers'?

Dinos cómo sobrevivir a nuestra locura. Kenzaburo Oé, el gran escritor japonés, premio Nobel de Literatura, captó en el título de un fantástico libro de relatos la esencia de nuestra era. Vivimos tiempos de locura y también de velocidad. Esa es la tecnológica promesa de la célebre red inalámbrica 5G. Aseguran –quienes de esto saben– que será cien veces más rápida que la actual. **Una película de dos horas se podrá descargar en menos de cuatro segundos.** El hombre tendrá la sensación de que el planeta jamás ha orbitado tan rápido. La velocidad hará casi instantánea la respuesta de un ordenador entre la orden que recibe y su ejecución. El Internet de las Cosas lo conectará todo. Desde el encendido de la casa hasta las bombas de diálisis o el rítmico latido de un corazón gobernado por un marcapasos. La velocidad será nuestra locura. Y **resultarán habituales los cirujanos a distancia, las armas hipersónicas, los coches autónomos** deslizándose por autopistas donde nadie toca un volante. Los números, claro, acompañarán a Kenzaburo Oé en su «locura». Algunos trabajos estiman que el 5G bombeará a la economía del planeta 12 billones de dólares en 2035. El mundo cambiará. Será distinto. Si creemos en esta dinámica, es la amanecida de la cuarta revolución industrial; si creemos en otros mañanas, será la alborada de la fragilidad.

Esta tierra hiperconectada también es un blanco enmarcado sobre luces rojas para los ciberataques. Pues si casi todo está unido, casi todo resulta susceptible de tener un eslabón débil. Solo hay que imaginar el daño que puede hacer un *hacker* que rompa la seguridad de una presa, los códigos que dan latido a un marcapasos o los algoritmos que guían un coche autónomo. La debilidad del álgebra, dirán algunos, y recitarán palabras. ***Malware, ramsomware, cryptojacking.*** El inglés tiene innumerables términos para describir esta amenaza consciente de que lo que no tiene nombre no existe. «El 5G no solo son frigoríficos conectados. Son cultivos agrícolas, son aviones, coches; todas esas cosas que actualmente pueden matar o

que permiten que alguien entre en la red y haga lo que quiera. Es una amenaza nueva frente a todo lo conocido anteriormente», alerta en la revista *The New Yorker* **Robert Spalding**, miembro del Consejo de Seguridad Nacional de Estados Unidos.

El FBI ha reconocido que el espionaje chino «es la mayor amenaza de contrainteligencia que afronta Estados Unidos»

El riesgo del cibercrimen es cada vez mayor y cada vez más violento. Toda esta debilidad está conectada a increíble velocidad a través de la red 5G. Hay preocupación en las empresas. Al menos en las que son conscientes del desafío que trae, también, la prosperidad tecnológica. La consultora Gartnet –muy atenta a estas disrupciones de la economía y la vida– estima que **solo este año se gastarán 124.000 millones de dólares en seguridad.** Otra consultora, Capgemini, ha descubierto que al mismo tiempo que crece el negocio digital, los riesgos de vivir ciberataques aumentan exponencialmente. En 2018, el Instituto Capgemini Research entrevistó a 850 ejecutivos sénior de siete sectores clave: productos de consumo, retail, banca, mundo del seguro, automoción, utilities y telecomunicaciones. El 21% de estos profesionales comentó que sus empresas habían sido atacadas y como consecuencia se produjo una brecha digital. El pago al barquero es alto. Un 20% afirmó haber perdido más de 50 millones de dólares. Vivimos en un gozne. «Nos encontramos ante un punto de inflexión que redefinirá la conectividad en la próxima década, por lo que ciudadanos, empresas privadas, ciudades y naciones deberían empezar a poner en práctica y desplegar las estrategias de ciberseguridad teniendo en cuenta que, a partir de ahora, debemos ver la foto como un todo», reflexiona **Javier Aznar**, senior manager de ciberseguridad de KPMG España.

El mundo se conecta también por sus desafíos y problemas. El 26 de marzo algo muy importante pasó casi inadvertido en el Viejo Continente. La Unión Europea publicó una recomendación dirigida a garantizar la seguridad de la red europea de 5G. No estaba escrito en el texto pero resulta fácil inferir que el organismo llamaba a protegerla frente a China pero también frente a Estados Unidos. Porque Europa está sola en este reto. Debe buscar sus propios recursos. Desde luego, que Huawei, el fabricante chino de bienes electrónicos y equipos de telecomunicaciones, fundado en los años ochenta por Ren Zhengfei, un ingeniero que empezó su carrera en el Ejército de Liberación del Pueblo, sea además el líder mundial en tecnología 5G trae de todo menos tranquilidad. **Tanto Reino Unido como Estados Unidos han acusado a la teleco china de espionaje.** El FBI ha reconocido que el espionaje

chino «es la mayor amenaza de contrainteligencia que afronta Estados Unidos». Y el ultimátum no es democrático. Se reparte de forma desigual. Los expertos del banco de inversión Goldman Sachs identifican a la banca como el sector más propenso a los ciberataques. Al fin y al cabo, maneja el material con el que está construido el mundo del siglo XXI: información y dinero. Quién lo duda, la partida está amañada y los dados, cargados. «Los *hackers* no están sujetos a ningún tipo de aprobación regulatoria y van por delante de las empresas, y, además, el uso de la inteligencia artificial ha redoblado el desafío», advierte el coloso de la inversión.

La red 5G exige incorporar 'ciberdefensas' desde su concepción original, según los expertos

Este universo hiperconectado es tan fascinante como el de verdad, y también se viven paradojas. Quizá no relacionadas con el espacio-tiempo pero sí con la simbiosis entre tiempo y trabajo. El investigador **Jonathan Spira** calcula que las distracciones (teléfonos inteligentes, redes sociales) producidas por el exceso de información y las interrupciones le cuestan a la economía estadounidense un billón de dólares al año. Con la red 5G, que **aumenta casi en cien veces la velocidad de conexión** frente a los sistemas anteriores, esa cifra podría quedarse corta. Y cuanto mayor es el volumen de datos circulando, mayor es la posibilidad de una grieta.

¿Un paraíso para los *hackers*? El tiempo dictará respuesta. Lo que parece claro es que la red es aún un modelo por armar. **Beatriz Castro**, consultora del área de finanzas de Analistas Financieros Internacionales (AFI), alerta de la incertidumbre de esos espacios en blanco. «El 5G, a diferencia del 4G, está diseñado para elegir qué tipo de conexión debe tener prioridad, es decir, serán las operadoras quienes elegirán entre una u otra. Esto podría provocar asimetrías en el mercado, pues habría que escoger, por ejemplo, si tienen preferencia las conexiones de seguridad nacional, las de servicios de hospitales…». La solución a este problema puede que se llame *slicing*. O sea, **dividir la red en otras más pequeñas para evitar la confrontación**. Todo esto debería generar preocupación. Pero, de momento, el miedo es una ciudad lejana tras el horizonte. «Por ahora, el 5G es un tema que no nos afecta. Los clientes no están pidiendo más información de la que ya se conoce ni forma parte de las pólizas de las aseguradoras», desgrana **Jacqueline Simón**, *manager* de Riesgos Financieros y Profesionales en el bróker asegurador Marsh. La situación, claro, puede cambiar, pues si de algo estamos seguros sobre el futuro es de que no está escrito.

En cuanto al presente, la mayoría de los grandes operadores estadounidenses planean migrar sus servicios a la parte más alta del espectro, donde las bandas resultan más anchas y permiten que fluyan por ellas torrenteras de datos. Aunque antes de llegar al techo habrá que pensar en la solidez de los cimientos. «Este tipo de proyectos no se conciben sin contar con la seguridad desde las capas más tempranas de diseño, no solo a la hora de garantizar que los dispositivos y redes que se despliegan ofrezcan protección contra posibles espionajes nacionales o continentales, sino que desde su concepción debe garantizar la seguridad de toda la arquitectura tecnológica de la que forma parte», asume Javier Aznar, de KPMG. Dicho de otro modo, **la red 5G debe incorporar ciberdefensas desde su concepción original.** Porque cada vez habrá más riesgo, más presión, más intereses, más fragilidad en un mundo que ha transformado las guerras comerciales en la Guerra Fría del siglo XXI. Dinos, Kenzaburo, cómo sobrevivir a nuestra locura.

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ.

Fotografía: Ethic

Fecha de creación
2019/09/25