Samuel Álvarez
Ingeniero de Telecomunicación. TEDxTALK Speaker

El dilema de la seguridad
5G da alas a IA e IoT, un cóctel que hay que controlar

La llegada de la tecnología 5G va a permitir un desarrollo incluso más amplio y 'poderoso' del resto de tecnologías habilitadoras digitales. El desarrollo de la Inteligencia Artificial está llegando a 'su adecuado punto de cocción', y el Internet de las Cosas casi ya posibilita que 'todo' hable con 'todo'. El cóctel está servido, un combinado que será difícil de controlar según en qué manos caiga. La seguridad va a ser para todo el mundo el principal caballo de batalla y será preciso elaborar un código ético que defina las líneas rojas y límites de su utilización.

Hace ya la friolera de más de tres décadas se estrenó una película de culto, cuyo guion se basaba en la idea de que una red inteligente, de máquinas conectadas, tomaba el control del sistema y aniquilaba a la humanidad. En aquella época era eso, ciencia ficción; una alucinación lejana y qué menos que imposible teniendo en cuenta el estado de la técnica en aquel momento.

Si hoy en día volvemos a revivir la película, con nuestro análisis ingenieril, de forma crítica y vehemente, y analizamos la viabilidad de la situación, es probable que ya no se nos dibuje una risa burlona en el rostro con la expresión de imposibilidad, y más bien nos entre un ligero escalofrío respecto a cuán real y cercano podría estar ese escenario, conociendo el estado de la técnica y la tecnología que ahora tenemos.

Evidentemente, por un lado, se requiere de un ingrediente de Inteligencia Artificial (IA), que quizás hoy no tengamos en "su adecuado punto de cocción", a pesar de que hay sistemas que deban ser apagados literalmente, porque han inventado un lenguaje para hablar entre ellos que el ser humano no comprende. O sistemas de IA que reproducen una obra artística a al que un experto tasador no podría diferenciar de la pieza original. Es decir, vamos por ese camino; cuánto quede, quizás ahora no se sabe, pero lo que sí está claro, es que no mucho, o, al menos, ahora sí lo creemos viable y posible. Y como las desdichas nunca vienen solas, a esta situación hay que sumarle otro punto rojo: el absoluto desgobierno o existencia de código ético que defina las líneas y límites a partir de las cuales se blinde el libre albedrío de un sistema de IA.

Por otro lado, tenemos un acrónimo que ha inundado nuestras vidas de forma desbordante, el querido `Internet de las Cosas´ (IoT). Ríos de tinta se han escrito sobre él, y lo que te 'rondaré morena'. Posibilidades del perfecto control de sistemas, máquinas y elementos electrónicos; todos gobernados al compás de un director de orquesta refinado, descentralizado y con capacidad de pulsar acordes imposibles que mueven miles, millones de elementos al son de la melodía que se requiera representar. Un director de orquesta, entusiasmado con que el movimiento sutil de sus manos haga sonar al unísono millones de yottabytes sin distorsión o desafine alguno. Todo hiperconectado, confiando en que los canales de comunicación y medios de transmisión nunca fallen, nunca colapsen y nunca, jamás, puedan manipularse. Tiene gracia, porque ya sabemos que esto hoy en día es posible, y lo seguirá siendo, solo que ahora, con tanta "cosa conectada", con más difícil gobierno y gestión.

Finalmente, y para rematar este cóctel de acrónimos que conforman un "eje del mal", tenemos la quinta generación de las comunicaciones móviles. La carrera hacia 5G comenzó hace muchos meses y todos los participantes tienen ya en su visión la línea de llegada. Pero aún se encuentran lejanas cuestiones preocupantes que no son baladíes, debido a que los participantes de la carrera se pierden solo en el ímpetu y la excitación social, industrial y económica que nos impulsa a la nueva era digital de la quinta generación. Pero ¿alguien está pensando en la ciberseguridad de este mundo tan hiperconectado y de tiempo real, cuando aún esta cuestión sigue siendo una realidad sin control para la situación tecnológica que tenemos en vigor actualmente?

La brecha de seguridad existente, ubicada entre la propia capacidad tecnológica del 5G y la capa de servicios que se apoyan en anchos de banda de vértigo y en latencias imperceptibles, resulta demasiado grande para que hoy en día se cante victoria.

Durante nuestro paso por la ingeniería y la universidad, muchos de nosotros vimos, disfrutamos y sufrimos diversos y variados conceptos aplicados a las telecomunicaciones. Pero en concreto aprendimos uno de forma efectiva y que se aplica a todos los ámbitos de la vida y por supuesto a nuestra profesión: si la entropía sube, la incertidumbre asciende; y si la incertidumbre asciende, el riesgo también lo hará. Por lo tanto, la conclusión evidente es que habrá que poner nuevos y mejores mecanismos y herramientas que ayuden al buen control y gobierno del riesgo, así como plantear qué reglas ayudarán a resolver, mitigar o recuperar situaciones de riesgo consumado.

El 5G sin duda marcará un antes y un después en cuestiones de calidad de servicio hiperconectado. Aunque lamentablemente, y si no enfatizamos la necesidad de la ciberseguridad, también marcará el sufrimiento por nuevos y sofisticados ciberataques y vectores de daño, como la manipulación o alteración de servicios y sistemas de conducción automática o los servicios prestados mediante la interacción hombre-máquina que se realizarán a distancia. Y esto sin entrar a abordar las cuestiones de privacidad de las personas, cuestión que deberá ser contada en otra historia.

¡Ah!, y por si alguien dudada de la película… era "Terminator". ■

Si la entropía sube, la incertidumbre asciende; y si la incertidumbre asciende, el riesgo también lo hará

Si no enfatizamos la necesidad de la ciberseguridad, el 5G también traerá nuevos y sofisticados ciberataques y vectores de daño