Inteligencia artificial, 'Big Data' y realidades digitales:

¿Las nuevas armas del director de seguridad?

Alfonso Castaño García / Vicepresidente de ASIS España

Si hay tres tendencias de las que todo el mundo habla en torno a la seguridad operativa en estos momentos son la inteligencia artificial, el *Big Data* y las realidades digitales. Pero como casi siempre sucede en este mundo, ni son tan nuevas, ni significan en sí mismas un paso decisivo para la seguridad tal y como hoy las entendemos. No dejan de ser unas nuevas herramientas en este gremio, pero de las que se precisa del artesano más hábil para sacar el mejor partido.

Inteligencia artificial

La inteligencia artificial (AI, por sus siglas en inglés) engloba un conjunto de acciones automatizadas que permiten la gestión de incidencias de un modo predictivo, en el que la enseñanza de esta metodología parte de un estudio de patrones de comportamiento y entorno realizados por una maquina siguiendo e imitando el comportamiento humano.

Cualquiera que haya tenido oportunidad de conducir un coche automático moderno habrá notado que éste realiza los cambios siguiendo su estilo de conducción. Si el conductor es tranquilo, cambiará a pocas revoluciones por minuto, y si es agresivo apurará las marchas. Como ven, nada nuevo tecnológicamente hablando, si bien ahora es cuando estamos viviendo la madurez de este tipo de tecnologías en nuestro sector.

Concretamente en el mundo de la seguridad, la AI está asentándose como una mejora sustancial de la analítica de video, y a este respecto me gustaría aclarar una duda que me plantean muchas veces: ¿qué es analítica y que es AI? El análisis, por definición, es el estudio de una situación y sus conclusiones son estadísticas. Si miramos cuántos coches circulan por una autovía, podemos clasificarlos por tamaños, contarlos y medir sus velocidades, incluso fijar zonas donde no deban estacionarse y que nos dé una alarma cuando esto suceda.

Evidentemente a medida que el patrón se vuelve más anómalo, más y mejor trabaja la analítica. Un vehículo en sentido contrario de la marcha será realmente fácil de detectar para la analítica más básica, ya esté instalada en la cámara o en un sistema. ¿Pero qué me dicen de buscar todos los monovolúmenes blancos que circulen por el carril central de una autopista en un periodo de tiempo determinado? Aquí es donde cobra sentido la inteligencia artificial, y este dilema puede complicarse aún más cuando buscamos que sea de una marca concreta o que lleve un número de ocupantes determinado.

La AI permite fijar un patrón de búsqueda sobre una trama de video procesada, de minutos u horas, y establecer los filtros de búsqueda que hayamos definido, mostrarnos los resultados coincidentes e incluso nos permite compararlos con otros similares para llegar a identificaciones definitivas, lo mismo que hacemos cuando buscamos a alguien entre la multitud con nuestro ojo y nuestro cerebro.

¿Fantástico verdad? Bien, antes de que se froten las manos ante tan buena nueva, he de decirles que el estado actual de la tecnología solo permite realizar con efectividad este proceso en forense, es decir, sobre grabaciones ya realizadas, que no es poco. Y como toda nueva medicina, tiene sus efectos secundarios y sus contraindicaciones.

El primer efecto secundario es la necesidad de utilizar servidores muy potentes para gestionar el enorme caudal de información que se procesa. Volviendo al ejemplo de la autopista, imaginen el número de coches que pueden grabarse en movimiento en una hora punta.

Esto nos lleva (al menos para mí como director de seguridad) a volver a encontrarnos con nuestras raí-

Foto: Soluciones Globales de Seguridad Electrónica.


Foto: Soluciones Globales de Seguridad Electrónica.

ces. Los que peinamos canas recordamos cuando grabábamos en un *time lapse* por multiplexacion, rezando para que se grabara justo el incidente y que no se perdiera mucha información cuando se saltaba de cámara. Después, con la grabación digital, comprendimos qué debíamos seleccionar, qué cámaras, en qué horas y siempre por detección de movimiento para poder aprovechar al máximo esta nueva tecnología. Luego, el desarrollo del *hardware* nos "pervirtió" y perdimos el camino, y pasamos a grabar todo, todo el tiempo, fuera o no importante; era barato y posible, lo difícil era encontrar el incidente buscado cuando no se sabía en qué momento había ocurrido, obligándonos al tedioso visionado de horas y horas de video grabado.

Bien, pues para aprovechar plenamente esta nueva tecnología debemos volver a los orígenes, ya que no es recomendable, ni técnica ni económicamente, dotar de inteligencia a un parque de 500 cámaras o procesar días completos de grabación, ni hacerlo en aquellas en las que prácticamente no hay movimientos que grabar durante horas.

Las contraindicaciones: para buscar algo existen los metadatos, la información que se graba en el sistema conjuntamente con la imagen, base de nuestras búsquedas como el color y la forma, y que provienen de las cámaras. Si éstas no son capaces de ver en color en condiciones de escasa iluminación o han conmutado a blanco y negro al activar sus focos leds, tan comunes hoy día, las búsquedas por similitud o color serán erróneas. Del mismo modo, si la calidad es mala, ya sea por resolución de una cámara o porque el sujeto está tan lejos que su imagen ocupa un puñado de pixeles, tampoco funcionara; se necesitan cámaras con 2 megapíxeles mínimo y un plano en el que el sujeto ocupe una porción de la imagen.

Conclusión: sea cual sea el sistema de AI empleado, precisa y mucho de una definición del director de seguridad, así como de un conocimiento de lo que es posible y lo que no es aconsejable. También deberá evaluar la arquitectura de la solución, en la que realmente solo hay dos modelos disponibles: las plataformas abiertas que trabajan con el flujo de video de cualquier fabricante, ideales para los entornos en los que ya hay desplegado un CCTV operando correctamente, o las cerradas, que lo hacen solo con cámaras de su propia marca, una opción a considerar cuando se va a renovar una instalación obsoleta.

'Big Data'

En cuanto al *Big Data*, o si lo prefieren (a mí me agrada más) con el término español "minería de datos", actualmente solo el 8 por ciento de los datos grabados por nuestros sistemas se procesan y estudian. Si trasladamos esta relación a cualquier otro ámbito de la vida, sin duda nos parecería un despropósito, con un gasto en recursos necesitado de una optimización urgente.

Al igual que cuando observamos una escena, nuestro cerebro procesa lo que nos ha llamado la atención, pero también capta otras situaciones que borramos de nuestra mente, si bien con una búsqueda específica las podemos encontrar. Lo hemos visto una y mil veces en las películas, cómo con técnicas de hipnosis es posible recuperar esa información, esos metadatos.

La minera de datos es eso, poder disponer de esos metadatos que viajan por las redes como secuencias de 1 y 0, sin ocupar casi espacio físico en los discos duros de nuestros sistemas, y clasificarlos para poder obtener una información. De hecho, como hemos visto la inteligencia artificial los utiliza; ahora el problema reside en qué queremos saber.

Permítanme ilustrar esta idea con un ejemplo. Una guía telefónica trae millones de datos que puedo clasificar por orden alfabético, incluso podría hacerlo por calles, pero si necesito hacerlo por edades y proximidad a un centro comercial –por razones de marketing, por ejemplo– necesitaría poder cruzar esa base de datos con la del padrón y con una de geoposición de este centro. Con la seguridad pasa lo mismo, tenemos ya los datos, pero necesitamos definir qué cruces y con qué base de datos nos va a producir resultados útiles. Aquí estoy hablando únicamente del punto de vista de la seguridad operativa, no de otras aplicaciones de la seguridad para procesos o estudios de mercado.

Para el director de seguridad de un aeropuerto, poder cotejar el número de personas que están en una terminal de salida con la cantidad de personas que han volado puede darle un dato muy útil de los posibles ladrones de tiendas que hayan actuado ese día; sin embargo, para el policía de aduanas será mucho más útil poder cotejar vestimentas anómalas al clima o al entorno de la terminal. En ambos casos el metadato ya está ahí, solo hay que buscarlo aunque de diferente manera.

Sin duda, de las tres tecnologías de las que hablo en este artículo ésta forma parte del presente actual. Entonces, ¿por qué no es de uso masivo? Pues porque las diferentes leyes de protección de datos vigentes actualmente entienden que una sucesión como 1000100001 es un dato personal, en vez de un cifrado algorítmico que precisa ser descifrado para, a mi modesto entender, ser considerado como tal.

Ya hemos echado un ojo al presente, ahora hablaremos del futuro inminente.

Realidades digitales

Bajo este epígrafe se comprenden varias tipologías que están unidas por el nexo común de referirse a un entorno generado mediante tecnología informática, que crea en el usuario la sensación de estar inmerso en él. Tampoco es el hallazgo de hoy. Sus primeros pasos datan de los años sesenta, si bien no fue hasta los noventa cuando los fabricantes de videojuegos se fijaron en esta tecnología, para definir una nueva familia de productos que, por razones comerciales, pocos juegos disponibles o técnicas (no era fácil de instalar), se olvidaron hasta la segunda década de este siglo, donde el desarrollo del *hardware*, mucho más potente y compacto, permitió la implantación masiva que actualmente se está coronando con los *Smartphone*, que han "democratizado" esta tecnología y que, tras lo visto en la última edición del Mobile World Congress, van a popularizar el uso de avatares (representaciones digitales de nuestro yo o del yo que quisiéramos ser).

La **realidad aumentada** se utiliza para crear una visión irreal de un entorno físico real a través de un dispositivo tecnológico, donde elementos físicos tangibles (una edificación o un entorno) se combinan con elementos virtuales (una explosión, un incendio…); es decir, sobre la realidad material del mundo físico se crea una realidad visual generada por la tecnología en la que el usuario percibe una mezcla de las dos realidades.

La realidad aumentada explora la aplicación de imágenes generadas por ordenador en tiempo real a secuencias de vídeo como una forma de ampliar el mundo real, y puede ser almacenada y recuperada como una capa de información en la parte superior de la visión del mundo real.

La **realidad virtual** es un paso más allá, en el que el usuario se sumerge totalmente en una experiencia virtual. Se aísla de la realidad material del mundo físico para sumergirse en un escenario o entorno producido informáticamente, que da la sensación de existir realmente.

Dirán los lectores, "¿y esto que tiene que ver con la seguridad?" Bien, se imaginan poder convertirse en un peligroso terrorista usando un avatar, burlando los sistemas de intrusión y poniendo a prueba los sistemas contraincendios y las barreras de contención de la instalación que protegemos y que tan bien conocemos, generando un videodocumento con escalas de tiempos, en el que se puedan evaluar errores y aciertos de nuestra planificación desde nuestro ordenador y despacho, sin poner en riesgo ni instalaciones ni vidas. ¿Sería fascinante verdad? Pues la realidad aumentada nos permite hacerlo.

Y ya puestos, por qué no tratar de planear una posible evacuación masiva ante un terremoto de un lugar emblemático en el que nunca hayamos estado. Con la realidad virtual sería posible.

Aquí estamos igual que los fabricantes de videojuegos en los años noventa. Nos faltan juegos, en este caso programas de simulación, y mejorar el *hardware*. Hoy necesitamos gafas, guantes y sensores, pero no duden de que lo vamos a ver en los próximos años. Vendrá de la mano de los actuales fabricantes de VMS, cuando conviertan sus analíticas plataformas de gestión en auténticos videojuegos, con la misma o mayor potencia, pero bajo un entorno más amigable y natural para la generación de "smart adictos" que está naciendo.

Si el amable lector ha llegado hasta aquí, espero que mi prosa desprenda esta idea: cuanto más avanzan las tecnologías en materia de seguridad, más precisan ese "saber hacer" de las direcciones de seguridad. La tecnología es siempre una herramienta y precisa una dirección humana para sacarla partido, so pena de convertirse en un *gadget* más al que no se le da uso.

Bibliografía:

- ASIS International: *Dynamics*.
- Tarallo, M: "Analytics for Everyone", en *Security Management*. Noviembre, 2014.
- Albarracín, Pablo: "Visualización avanzada de datos: La belleza del Big Data", en *América Economía Tecno* (tecno.americaeconomia.com). Publicado: 12 de agosto de 2013.
- Web Mundo Virtual: www.mundo-virtual.com S

Foto: Soluciones Globales de Seguridad Electrónica.