¿DEMASIADA TECNOLOGÍA?

La Tecnología ha sido un recurso fundamental para la especie humana, no solo para sobrevivir y permanecer sino prevalecer sobre el medio, al grado de desarrollar tal grado de dependencia que se podría decir que nos hemos convertido en un "homo tecnologicus". Por ello no hay campo en la vida del ser humano en que no esté presente y predominantemente actuante alguna forma de la tecnología, al grado de marcar el rumbo de su evolución y desarrollo. Y el ámbito de la Seguridad no escapa de este fenómeno. Sin embargo, esta dependencia, si bien ha aportado beneficios de progreso para la humanidad, también ha representado costos significativos, de tal suerte que se puede cuestionar si no se tiene un problema de demasiada tecnología.

La **Tecnología** es el resultado de los esfuerzos humanos para adaptar las condiciones "*naturales*" del medio, adversas y hostiles, a otras más favorables para propiciar y facilitar su bienestar (*satisfacción de necesidades*) y prosperidad (*logro de aspiraciones*). Asimismo, se tiene que todo recurso de tecnología detenta un perfil de **capacidades** (*qué puede hacer*) y **limitaciones** (*hasta dónde puede llegar*), determinado por su propósito de **funcionalidad** (*para qué sirve*), de tal suerte que se proyectan cuatro principios para su aplicación:

- **Posibilidad**. En Tecnología **casi todo es posible**, y si no existe, se puede construir. Sólo es una cuestión de tiempo y costo.
- **Factibilidad**. La Tecnología, por más sofisticada que sea, **nunca podrá ir más allá de su diseño y su programación**.
- **Debilidad**. Todo lo que la tecnología **puede hacer**, la misma tecnología u otra **lo puede deshacer**.
- **Neutralidad**. La tecnología **por sí misma no es buena o mala**, lo que se puede calificar como tal es el uso que se le da.

Por ello, toda aplicación de **tecnología** se conforma como un **binomio hombre-máquina**, en el que sus recursos sólo son herramientas que, en mayor o menor medida, **ayudan a hacer el trabajo, pero no hacen el trabajo**, y con el factor humano como el elemento consciente, responsable en última instancia de todo discernimiento y decisión, porque sólo éste factor es capaz de hacer frente a condiciones o situaciones imprevistas, ya sea adaptando lo d disponible a nuevas condiciones, o creando nuevas funcionalidades.

La naturaleza **dinámica y heterogénea** de la conducta humana, aderezada con atributos de complejidad y diversidad, redunda en una proclividad hacia lo imprevisible, ante lo cual se enfatizan las **limitaciones** derivadas de su perfil de **Carencia**s (*no se tiene lo que se*

necesita). **Deficiencias** (*lo que se tiene no funciona como se requiere*), e **Insuficiencias** (*lo que se tiene no alcanza para todo lo que se necesita*), o perfil **CDI**, que pueden provocar un efecto de **"ceguera"** ante condiciones no previstas, o bien de **"filtrado"**, cuando concurren condiciones no previstas con las condiciones previstas en la funcionalidad. Asimismo, las **posibilidades** pueden aventajar a las **debilidades**, con desarrollos tecnológicos sofisticados que puedan "**engañar**" incluso a las funcionalidades de corte heurístico con aprendizaje automático sustentadas en aplicaciones de inteligencia artificial (*machine learning*), ya que suelen operar con base en los datos recopilados de eventos ocurridos, de tal suerte que podrían llegar a **evitar la recurrencia, pero no la ocurrencia inicial** de fenómenos inéditos.

En este orden de ideas, un caso de "*engaño*" podría ser la activación automática de un mecanismo de extinción de incendios en una fábrica de productos de papel, causada por un funcionamiento erróneo, incidental (por errores o falla) o intencional, del mecanismo de detección, lo que dañaría la materia prima o el producto terminado. Por otra parte, un caso de "*ceguera*" podría ser no detectar vía reconocimiento facial a un delincuente, porque el registro de sus facciones no se encuentre en la base de datos. Y un caso de "*filtrado*" podría ser la posibilidad de no detectar una situación de riesgo que ocurra dentro del alcance de una cámara pero fuera de su campo visual, por estar operando con un recorrido automático (*tour*) en posiciones predefinidas de cobertura (*presets*).

Las cada vez mayores facilidades que ofrecen los avances en tecnología propician una excesiva dependencia, olvidando al principio de **factibilidad**. En Octubre de 1962, la Unión Soviética emplazó Misiles Nucleares en la Isla de Cuba, con una manobra logística de camuflaje muy efectiva contra los vuelos de reconocimiento de los Estados Unidos, los cuales, a pesar de la avanzada tecnología fotográfica de la época, no mostraban de los militares soviéticos ni los equipos de lanzamiento. Pero un **analista humano**, al observar las fotografías, detectó un detalle que consideró como una anomalía: la construcción reciente de campos de futbol en un entorno de afición al beisbol. A partir de este detalle, modificaron la forma de los vuelos de reconocimiento y descubrieron las instalaciones de los misiles, detonando la Crisis de los Misiles de Cuba.



El 26 de septiembre de 1983 el Sistema Satelital de Alerta Temprana de la Unión Soviética alertó del lanzamiento de misiles desde los Estados Unidos, lo que ameritaba una respuesta inmediata de contraataque nuclear. Sin embargo, el **Teniente Coronel Stanislav Petrov**, oficial a cargo del sistema, pareció ver una anomalía en tal alertamiento, imposible de confirmar por el sistema de radares, pero que efectivamente era producto de un mal funcionamiento, y no activó la respuesta programada. Posteriormente se determinó que la

falla fue resultado de una condición ajena al sistema, una peculiar coincidencia de la posición relativa del sol reflejada en las nubes a gran altura había sido interpretada por el sistema como la señal de misiles volando hacia el territorio soviético. Esto fue conocido como el Incidente del Equinoccio de Otoño.

Estos ejemplos evidencian que la **consecuencia** de las limitaciones y debilidades de los recursos tecnológicos es la posibilidad de causar **efectos no deseados** (*daños y/o perjuicios*), por la **activación o contención "*automatizada*"** de alguna acción **sin opciones oportunas de anulación o reversión**. Las tendencias actuales de dependencia de fuentes de información ubicadas en sitios con alto potencial de accesos hostiles no autorizados (como el *cloud computing*), intensifican estas posibilidades de riesgo. Y en el campo de la Seguridad, esta consecuencia puede proyectar repercusiones **críticas**, en virtud de que un error puede provocar **alguna pérdida, incluso de vidas**. Por ello, **la tecnología puede ser muy conveniente, pero siempre será insuficiente** por sí misma, porque solo el factor humano es capaz de discernir y decidir con información incompleta, confusa y muchas veces aparentemente contradictoria. Y **demasiada tecnología, al nivel de adicción, puede llegar a ser inconveniente**.

Nada con exceso, todo con medida
Solón

David Chong Chong

Ingeniero en Comunicaciones y Electrónica, egresado de la Escuela Superior de Ingeniería Mecánica y Eléctrica del Instituto Politécnico Nacional. Diplomado en Reingeniería de Procesos por el Instituto Tecnológico y de Estudios Superiores de Monterrey. Master en Ciencias de la Seguridad por la Universidad Internacional de Seguridad (UNIVERIS) y CEAS Internacional. Secretario General para México de la Corporación Euro Americana de Seguridad, CEAS México. www.ceasmexico.org.mx Correo electrónico: dchong@ceasmexico.org.mx