>> Jorge Dávila

Los próximos diez mil *tuits*

Todos los principios de año se llenan de buenas intenciones y de cábalas sobre lo que tenemos delante, sobre lo que puede ocurrir; pues bien, el mundo de las tecnologías de la información y de la seguridad no tiene por qué ser distinto. En la columna de este primer número de 2016 intentaremos ver qué puede depararnos el futuro a medio plazo.

Corría el año 1973 y Adrian Berry escribía su obra "*Los próximos 10.000 años: el futuro del hombre en el universo*" [1]. Aquellos eran tiempos arrogantes en lo tecnológico y aeroespacial, se respiraba una gran euforia respecto al porvenir tanto inmediato como lejano. Había estallado el optimismo y el entusiasmo de 1969 [2], y Occidente se sentía imparable avanzando como una locomotora hacia un maravilloso futuro.

En la película "*2001, una odisea del espacio*" (rodada en 1964 y 1968) los dos grandes maestros Kubrick y Clarke presentaban una visión pretendidamente realista del futuro a treinta y tres años vista. Para ello habían contado con bastantes asesores y, sin embargo, se equivocaron radicalmente. Todavía hoy nadie viaja a Jupiter o a Saturno, desde luego no hay colonias lunares y el entrañable pero nada empático HAL 9000 [3] no existe. Ni siquiera hay un impenetrable monolito enterrado en la Luna. Esta vez la ficción superó a la realidad cosa que, por otra parte, es lo que ocurre casi siempre.

Caído el muro de Berlín, estigmatizada la Unión Soviética, desaparecida la Guerra Fría, los misiles dejaron de ser urgentes e incluso útiles, y la aventura aeroespacial cayó en picado en cuanto a su protagonismo social y financiación. Mientras tanto, la microelectrónica, que había crecido a la sombra de aquellos erectos segmentos fusiformes, terminó colonizando la Tierra.

Sin que la mayoría de los pobladores del primer mundo tengan muy claro cómo hemos llegado a esto, el caso es que los niños de doce años no conciben que hubiese un tiempo sin teléfonos inteligentes, sin tabletas, sin GPS, sin cobertura 3G incluso subterránea [4], y sin ese éter que todo lo envuelve y que ellos llaman WiFi.

Los experimentos como ARPANET [5] establecieron los principios de una red basada en la conmutación de paquetes [6] y la primera implementación del protocolo TCP/IP [7], que son la esencia de las "*redes telemáticas*" que son la base de Internet [8]. Los últimos veinte años los hemos gastado en desarrollar aún más esa idea original y, sobre todo, en **fomentar que toda la sociedad occidental se empape de esas tecnologías hasta el punto de no poder existir sin ellas**.

Con la llegada de la nueva esencia, vinieron las nuevas materializaciones de los riesgos ya antiguos, y éstos crecieron a espaldas de una sociedad endemoniadamente narcisista. Su vitalidad se plasma en cosas tan etéreas como las "redes sociales" [9] y los expositores de vidas privadas que son Facebook, Twitter o Instagram. Mientras tanto, información de todo tipo, la del negocio bancario, la de las Administraciones y Estados abrazaban la nueva tecnología.

CIBERCRIMEN: SE SUBE EL TELÓN

Paralelamente, los que sabían descubrir fallos, errores de diseño y chapuzas varias en el software que da cuerpo a esa ilusión, dieron paso al Cibercrimen y a su muy lucrativa economía. Fueron necesarios más de diez años para que Occidente se diese cuenta de que precisaba inventar la Ciberdefensa, y desde entonces a todo se le añade el prefijo Ciber, venga a cuento o no tanto.En este punto es muy difícil enfrentar el reto de imaginar cuáles serían los temas tratados en los próximos diez mil *tuits* de un gurú o avezado bloguero tecnológico especializado en temas de seguridad.

Terminal de usuario

Sin duda, el primer grupo se centraría en el más débil de los frentes de la informática moderna, que es **el terminal del usuario**. La fusión de la telefonía GSM y de los asistentes digitales personales (PDAs) [10] podría haber ido por el lado de proporcionar comunicación (oral, escrita

Los sistemas muy vigilados lo que hacen es legalizar la violación de derechos fundamentales, como son la vida privada, la libertad de expresión y el derecho a no sufrir, en lo esencial, discriminación alguna. Por otra parte, los sistemas inseguros anulan todos los derechos civiles y nos lanzan a los pies de los tiranos. En conclusión, si queremos seguir siendo civilizados, necesitamos menos vigilancia y más seguridad en los sistemas que nos rodean. Vigilancia y seguridad no son sinónimos, sino todo lo contrario.

[1] Adrian Berry: "The next ten thousand years: a vision of man's future in the universes" (London: Cape, 1974), ISBN 0-340-19924-5

[2] Rob Kirkpatrick: "1969: The Year Everything Changed" ISBN-13: 978-1616080556

[3] Ver https://en.wikipedia.org/wiki/HAL_9000

[4] Me refiero a las estaciones del Metro de Madrid que incluyen ese servicio a muchos metros por debajo del asfalto.

[5] ARPANET = The Advanced Research Projects Agency Network https://en.wikipedia.org/wiki/ARPANET

[6] Ver https://en.wikipedia.org/wiki/Packet_switching

[7] Ver https://en.wikipedia.org/wiki/Internet_protocol_suite

[8] En diciembre de 1974 se publica el RFC 675 "Specification of Internet Transmission Control Program" por los autores VintonCerf, YogenDalal, y Carl Sunshine, en donde utilizan por primera vez el término internet como abreviatura de "internetworking"

[9] Ver https://en.wikipedia.org/wiki/Social_networking_service

[10] Ver https://en.wikipedia.org/wiki/Personal_digital_assistant

y multimedia) asociada con funciones de autenticación e identidad digital. Sin embargo no fue así y venció el principio de libre adaptación a los caprichos del dueño. En lugar de comunicadores se hicieron máquinas "*de propósito general*" en las que se podía ejecutar prácticamente cualquier aplicación, desde monitores de fertilidad [11] hasta la saga Candy Crush [12]. Ese generalísmo ha abierto miles de canales de infiltración y exfiltración cuyo control se ha demostrado imposible incluso para clubs tan selectos como los App Store de Apple. La moda BYOD sólo viene a empeorar las cosas haciendo que el cencerro digital que permanentemente nos delata, encima lo estemos pagando nosotros.

Nube

Otro grupo sería el de **la Nube**, nombre nuevo de lo que antes era la externalización de servicios e infraestructuras. Las técnicas de virtualización ha transformado el antiguo menester de alquilar hardware, en algo "*soft*" que cualquiera puede emprender desde cualquier terminal. La presión no siempre bien intencionada por la adopción de este nuevo modelo de negocio, ha atropellado cualidades muy importantes como son la confidencialidad, la integridad y la propiedad de los datos digitales. Es muy difícil (imposible) creerse que algo que se sube a las nubes actuales sigue siendo confidencial, permanece inmutable o, simplemente, puede ser borrado. ¿Qué mejor prueba hay de la pérdida absoluta de control que el no poder borrar una información que uno suponía propia?

La corrección de los errores actuales en el diseño de la Nube, precisan un serio replanteamiento de las redes telemáticas [13] de principios de los setenta que seguimos usando. Quizás haya *tuits* llamando a la correcta compartimentación de las redes y la operación a varios niveles de las distintas informaciones que por ellas circulan. Quizás alguien difunda que si todos los problemas no son el mismo, tampoco tiene por qué ser la misma su solución.

Big Data

Otro de los temas tratados en esos diez mil *tuits* sería lo que hoy se llama **Big Data** [14], especialmente en lo que se refiere al control y monitorización de procesos o situaciones de interés empresarial o comercial. La explotación de ingentes cantidades de datos no estructurados con la promesa de encontrar verdaderas joyas informativas en ellos, es la promesa de "*El Dorado*" [15] para muchos que, por su actividad (proveedores de algún tipo de servicio) quieren estrujar [16] los datos que generan o tratan, de modo que con ello destilen un material nuevo que puedan vender a otros con un alto beneficio neto.

Vigilancia

Un tema que ya es importante y seguirá siéndolo en el corto y medio plazo es el de la **vigilancia** [17] **ubicua, inespecífica, automática y persistente** a la que ya se está sometiendo a las población del planeta. Quizá algunos de los futuros *tuits* hablen de algunos irredentos que estarán dispuestos a engañar al Gran Hermano. Con ellos nacerán tecnologías de **camuflaje digital**, no en el sentido textil que actualmente se le da [18], sino en el de cómo ocultar sitios, personas, activos, comunicaciones y procesos en lo vulgar, en lo mediocre, en lo frecuente. Cegar los ojos del Big Data será un sueño al que más de uno se consagrará en los tiempos que aún están por venir.

Con el aumento de las capacidades para analizar todo lo que hacen los individuos y descubrir su significado (correlación), algunos futuros *tuits* hablarán de **contravigilancia**, entendiendo por tal las prácticas que impidan la vigilancia o, al menos, la dificulten considerablemente.

Una posible respuesta a la amenaza del Gran Hermano es lo que se conoce como **vigilancia inversa**. Hoy en día consiste en individuos o grupos de ellos que vigilan a los agentes del sistema –por ejemplo policías antidisturbios metidos en faena–, para hacer públicos casos de brutalidad y otros excesos. En el futuro próximo esa corriente de autodefensa podrá darse también en el escenario digital, de modo que sean los sistemas de información propios los que se utilicen como arma contra su propietario. Este escenario muy bien podría ser el preferido frente a las empresas.

Mientras la sociedad abrazaba la nueva tecnología, los que sabían descubrir fallos, errores de diseño y chapuzas varias en el software que da cuerpo a esa ilusión, dieron paso al Cibercrimen y a su muy lucrativa economía. Fueron necesarios más de diez años para que Occidente se diese cuenta de que precisaba inventar la Ciberdefensa y, desde entonces, a todo se le añade el prefijo Ciber, venga a cuento o no tanto.

No huelga decir que la emergente IoT ni se plantea en serio lo de hacer que esos sistemas sean mínimamente seguros o, incluso, controlables. Lo sorprendente es que estas justificadísimas sospechas no están frenando la instalación de contadores inteligentes por toda Europa, sin que realmente se sepa quién los controla o quién puede terminar controlándolos.

[11] Ver http://appcrawlr.com/ios-apps/best-apps-fertility-awareness-method

[12] Ver https://en.wikipedia.org/wiki/Candy_Crush_Saga

[13] Ver https://en.wikipedia.org/wiki/Computer_network

[14] Ver https://en.wikipedia.org/wiki/Big_data

[15] Ver https://en.wikipedia.org/wiki/El_Dorado

[16] Ver https://en.wikipedia.org/wiki/Predictive_analytics

[17] Ver https://en.wikipedia.org/wiki/Surveillance

[18] Ver https://en.wikipedia.org/wiki/Digital_camouflage

IoT

Otro grupo de mensajes que podemos imaginar se difundan en un futuro medio en esos futuros *tuits* es el relacionado con la denominada **Internet de las Cosas** (IoT)[19]. Con este nombre hoy nos referimos a redes de objetos físicos o "cosas" que contiene elementos microelectrónicos, software, sensores y actuadores dentro de ellas; todo ello junto a capacidades de conexión (generalmente por radio), que les permite recoger e intercambiar datos y comandos. En este escenario los objetos físicos pueden ser monitorizados y controlados de forma remota a través de una red extensa. Sus defensores hablan de crear oportunidades para una mejor integración del mundo físico y los sistemas controlados por ordenadores, consiguiendo así mayor eficiencia, precisión y (sobre todo) beneficio económico. No huelga decir que **la emergente IoT ni se plantea en serio lo de hacer que esos sistemas sean mínimamente seguros o, incluso, controlables**. Lo sorprendente es que estas justificadísimas sospechas no están frenando la instalación de contadores inteligentes[20] por toda Europa, sin que realmente se sepa quién los controla o quién puede terminar controlándolos.

Llevables (*Wearables*)

También podremos ver *tuits* consagrados a los muy inseguros y perfectos enemigos de la intimidad que son los llevables (***wearables***)[21]. Es mucho el esfuerzo que están haciendo los fabricantes de chips[22] para conseguir computadores completos tan pequeños como un grano de arroz[23]. Una vez que lo consigan –y falta poco–, habrá una presión difícilmente resistible para incluirlos en absolutamente todas partes. Por ahora nos salva el problema de la energía para alimentarlos, pero la capacidad de las nuevas baterías y sobre todo de los **supercondensadores**[24], avanzan incluso más deprisa que el diseño y la realización de los propios chips.

Objetos ciberfísicos

El siguiente paso evolutivo de la actual domótica[25] vestida de IoT, es lo que algunos llaman **objetos ciberfísicos**[26]. En este caso, en lugar de hablar de un elemento autónomo que se relaciona con otros por radio; los objetos ciberfísicos se diseñan como una red en sí, compuesta por diferentes elementos físicos con capacidades sensoriales y de respuesta. Estos objetos son la evolución conjunta de la robótica y las redes de sensores[27] a los que se les quiere añadir cierto grado de "*inteligencia*" (más bien de control) encaminados a conseguir un fin. Estos sistemas dispondrían de una alta adaptabilidad, autonomía, eficiencia, funcionalidad, confiabilidad, seguridad física, y usabilidad.

Ejemplos de ellos los podemos encontrar en el sector automovilístico con sus sistemas anti-colisión, en la cirugía robótica[28] y en la fabricación nanométrica, en los sistemas de manipulación de materiales peligrosos o en las operaciones en entornos hostiles (sistemas de búsqueda y rescate), en los sistemas automáticos de control aéreo, en la guerra robotizada[29], en la eficiencia energética –como en el caso de los "*edificios de energía nula*"[30]– y en sistemas de monitorización médica unida al dispensado automático de fármacos.

No pensemos que todo esto es ciencia ficción y que es parte de un discurso futurista: ya en el 2015 se han iniciado campañas contra el desarrollo y uso de robots asesinos[31], cuyos promotores si se han preocupado de aunar eficiencia de fuego y precisión de tiro, pero no tanto en la seguridad y control operativo de esos artefactos.

Siempre es difícil la tarea de la Sibila[32] pero es algo que no está de más hacer de vez en cuando. Es conveniente prestar atención a la evolución tecnológica en general, y de la información en particular, así como a los curiosos caprichos del mercado, que determinan quién sobrevive y quién se extingue. Es preciso hacerlo, ya que el precio que podemos terminar pagando como ciudadanos y usuarios es muy grande.

Los sistemas muy vigilados lo que hacen es legalizar la violación de derechos fundamentales como son la vida privada, la libertad de expresión y el derecho a no sufrir, en lo esencial, discriminación alguna. Por otra parte, los sistemas inseguros anulan todos los derechos civiles y nos lanzan a los pies de los tiranos. En conclusión, si queremos seguir siendo civilizados, **necesitamos menos vigilancia y más seguridad en los sistemas que nos rodean. Vigilancia y seguridad no son sinónimos, sino todo lo contrario**. ■

Con el aumento de las capacidades para analizar todo lo que hacen los individuos y descubrir su significado (correlación), algunos futuros tweets hablarán de contravigilancia, entendiendo por tal las prácticas que impidan la vigilancia o, al menos, la dificulten considerablemente.

[19] Ver https://en.wikipedia.org/wiki/Internet_of_Things

[20] Ver https://en.wikipedia.org/wiki/Smart_meter

[21] Ver https://en.wikipedia.org/wiki/Wearable_computer

[22] Ver http://www.intel.com/content/www/us/en/wearables/wearables-overview.html

[23] Ver http://www.popularmechanics.com/technology/a14950/worlds-smallest-computer-michigan-micro-mote/

[24] Ver https://en.wikipedia.org/wiki/Supercapacitor

[25] Ver https://en.wikipedia.org/wiki/Home_automation

[26] Ver https://en.wikipedia.org/wiki/Cyber-physical_system

[27] Ver https://en.wikipedia.org/wiki/Wireless_sensor_network

[28] Ver https://en.wikipedia.org/wiki/Robot-assisted_surgery

[29] Ver https://en.wikipedia.org/wiki/Military_robot

[30] Ver https://en.wikipedia.org/wiki/Zero-energy_building

[31] Ver https://www.stopkillerrobots.org/

[32] Ver https://en.wikipedia.org/wiki/Sibyl

[33] Ver https://en.wikipedia.org/wiki/Smart_meter

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es