Internet y nuevas tecnologías

Roberto Plá
Teniente coronel de Aviación
http://robertopla.net/

CIBERGUERRA

ATAQUE A LA RED ELÉCTRICA

No es necesario hacer un gran esfuerzo para entender que la desaparición de la energía eléctrica en nuestras vidas supondría una catástrofe inconmensurable. Desde la calefacción o la refrigeración, la alimentación o la conservación de alimentos, los hospitales y las comunicaciones, prácticamente todos los aspectos de la vida moderna pasan por la necesidad de electricidad.

Los grandes cortes de suministro causados por incidentes técnicos se recuerdan como grandes catástrofes y no es difícil encontrar sus reseñas en las noticias o en la Wikipedia.

Hace tiempo que se señalan como vulnerabilidades ante posibles ciberataques, los sistemas de ordenadores que controlan el tendido eléctrico. Aunque hasta hace poco se trataba solo de una posibilidad teórica, la aparición de un *software* malicioso con ese objetivo ha puesto el tema de actualidad.

Telvent fabrica el sistema de control remoto que gestiona las redes inteligentes usadas en parte del sistema eléctrico. El 10 de septiembre de 2012, Telvent informó a sus clientes de que habían descubierto que *hackers* habían penetrado en su cortafuegos interno y en su sistema de seguridad, robando detalles del producto de Telvent OASyS SCADA, el cual ofrece a las compañías eléctricas un puente entre la tecnología antigua y la nueva de redes inteligentes. El robo de informacion afectó a las operaciones de Telven en Canadá, Estados Unidos y España. En España, el sistema global de transporte de la corriente por las líneas eléctricas lo hace la empresa Red Eléctrica de España (REE) que, asimismo, es el operador del sistema.

En Estados Unidos, a principios de febrero de 2013, el presidente Obama dictó una orden ejecutiva de ciberseguridad que tenía por objeto ayudar a que la infraestructura crítica norteamericana resistiera los ataques informáticos.

Uno de los principales problemas es que la industria eléctrica nunca pensó que sus infraestructuras pudieran ser operadas maliciosamente, por lo que el aspecto de la seguridad no se contemplaba en el diseño. Debido a su fiabilidad técnica y robustez, estos equipos se renuevan muy de tarde en tarde, lo que dificulta su actualización.

Foto:Wikipedia

Con la llegada de la automatización, los sistemas de control están formados por: redes de ordenadores, *software* que controla los equipos, y por los elementos físicos muy específicos que permiten efectuar las operaciones de control en la red eléctrica. Un *software* malicioso, destinado a operar estos elementos de control de forma que provoque su inutilización debe ser capaz de iteractuar con los mismos, por lo que su programador debe conocer sus particularidades y sus vulnerabilidades, pero necesita también un elemento que le permita infectar y transportarse a través de redes convencionales esquivando las medidas de control y seguridad, en una forma similar a como realizó su infección y ataque el gusano Stuxnet.

La infraestructura y el conocimiento necesario para estas acciones no suele estar al alcance de un quinceañero superdotado o de unos estudiantes universitarios, por lo que la aparición de indicios de existencia de *malware* con esta misión hace pensar en el respaldo de gobiernos, bien sea para utilizarlo como armas o -si somos desconfiados- para probar las propias defensar o alertar/concienciar a la industria sobre las ciberamenazas.

Según la empresa de seguridad Symatec, “Intrusos informáticos han estado paseándose a sus anchas por las entrañas de un millar de instalaciones energéticas de 84 países de todo el mundo durante al menos el último año y medio.” Entre estos países se encuentran España, Estados Unidos y Canadá, siendo nuestro país, con un 27% de los ataques, uno de los más afectados. Las empresas del sector energético niegan haber sido objeto de esos ataques y Symatec no da nombres, pero sí detalles como que, aunque se centraron en el robo de información, si los atacantes "hubieran utilizado la capacidad de sabotaje de que disponían

podrían haber causado daños o interrupciones del suministro" o que los *hackers* eran rusos (por sus horarios) y que "borraron sus huellas".

En definitiva, ¿estamos ante un ataque real, que las víctimas intentan minimizar? O por el contrario ¿se trata de un señuelo lanzado por intereses comerciales o estratégicos para acelerar las inversiones en seguridad?. En cualquier caso el peligro y el riesgo existen y haríamos bien en preocuparnos por el tema.

http://delicious.com/rpla/raa836a

DISPOSITIVOS MÓVILES

DISPOSITIVOS "WEARABLES"

No es un concepto nuevo, pero hasta el momento actual no había sido nada más que algo experimental, solo apto para "frikis" muy fanáticos o *geeks* militantes. Se trata de los dispositivos electrónicos integrados en la ropa. Precisamente la expresión inglesa *wearables* quiere decir eso mismo: "vestibles", que te los puedes poner. La falta de una traducción precisa en español nos hace utilizar el término inglés.

Desde el punto de vista militar, tienen una enorme importancia. Tal y como me decía el otro día mi buen amigo Fernando Acero en la cafetería del Centro de Guerra Aérea: los teléfonos móviles, las tabletas o los *notebooks* no son relevantes en el panorama futuro de la tecnología militar, porque el combatiente necesita tener las manos disponibles.

También coincidíamos en que esta es una tecnología que no pertenece al futuro: es propia del presente, y a la velocidad con que se desarrolla pronto será una cosa del pasado. Quien no se haya subido a ese tren estará tan en desventaja frente a quienes dispongan de ella, como los indios con sus flechas frente a las ametralladoras. Así de sencillo.

Sin embargo, yo, que soy un nostálgico, quiero reivindicar la importancia de los teléfonos inteligentes y las tabletas, de los dispositivos que leen el movimiento de los ojos y traducen los impulsos nerviosos, del *software* OCR y el de dictado. Todas estas tecnologías están presentes de forma natural en nuestra vida cotidiana. Le dictas a tu teléfono mensajes que pueden recorrer varias veces el mundo antes de que levantes el dedo del botón 'enviar' y le muestras a tu cámara un letrero en cualquier idioma para que lo lea y te lo traduzca, te dejas guiar por el GPS integrado en el coche o en el teléfono chino que compraste a precio irrisorio por internet.

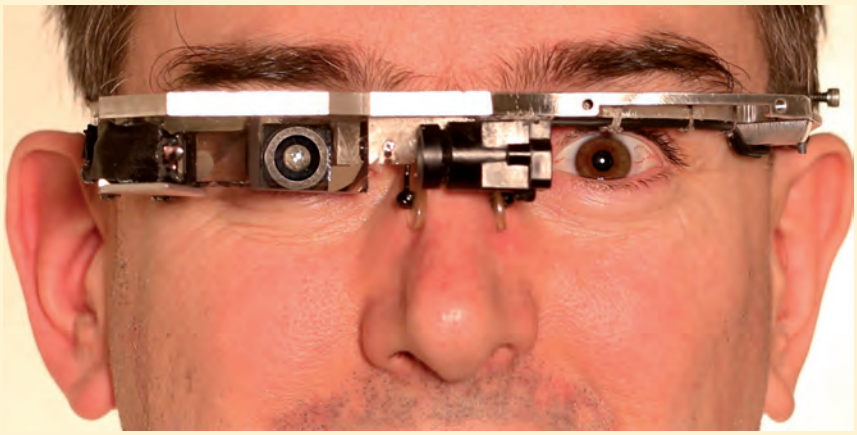

Foto:Wikipedia

Todas esas tecnologías que ahora nos parecen tan sencillamente integradas en nuestras vidas, andan en busca de una interfaz que deje libres nuestras manos y nuestros bolsillos o bolsos de aparatos pesados o ligeros para introducirse en nuestra ropa, los complementos de moda o en un nuevo tipo de peineta unisex. En los dispositivos que actualmente compramos como posesos, se desarrolla un experimento tecnológico. Las nuevas interfaces y las nuevas prestaciones de los programas más avanzados se prueban y se mejoran, al tiempo que se estudia su eficacia y aceptación para desarrollar una nueva generación de dispositivos.

Estar presente en el desarrollo de los dispositivos y del *software* que les da vida es una necesidad estratégica. Adoptar el papel de usuario, aceptar el rol de cliente como única participación en este mercado es tan suicida como elegir seguir cazando bisontes con lanzas para vestirse y alimentarse. Y esta es una conclusión aplicable al ámbito militar o al ámbito económico. Ya conocemos las consecuencias de la política del "que inventen ellos", no podemos repetirla.

http://delicious.com/rpla/raa836b

REDES SOCIALES

MANIPULANDO LAS MENTES

A finales del mes de junio la prensa publicó que durante una semana del mes de enero de 2012, la red social Facebook manipuló las cuentas de 700.000 usuarios para analizar la posibilidad de influir sobre sus emociones, en un experimento psicológico sobre "contagio emocional masivo virtual", sin la autorización ni el conocimiento de los usuarios.

Las graves implicaciones éticas que tal noticia implica se han saldado con una disculpa de la compañía que con menos respeto y discreción trata nuestros datos privados; y mientras los expertos se escandalizan sobre los posibles abusos que hayan podido producirse y de los que no se ha tenido conocimiento, y de las implicaciones de todo tipo que una acción como esta podría tener en aspectos tan críticos para la sociedad como la economía, el mercado, la paz social, o el propio ejercicio de la soberanía política, no parece que su conocimiento por parte de los usuarios haya derivado en abandonos masivos de suscripciones a la red social, de forma que la triste noticia no hace suponer que sea que los tiempos del Gran Hermano hayan llegado, sino que, al parecer, nos gusta.

http://delicious.com/rpla/raa836c

Enlaces

Los enlaces relacionados con este artículo pueden encontrarse en las direcciones que figuran al final de cada texto