ieee.es
Instituto Español de Estudios Estratégicos

Documento
Marco

09/2014 3 de julio de 2014

*Luis de Salvador Carrasco**

LOS PROBLEMAS ESTRUCTURALES EN EL PLANTEAMIENTO DE LA CIBERSEGURIDAD

LOS PROBLEMAS ESTRUCTURALES EN EL PLANTEAMIENTO DE LA CIBERSEGURIDAD

Resumen:

La ciberseguridad es un problema que implica a gobiernos, empresas y ciudadanos. La dependencia que todos los sectores sociales y económicos tienen de la infraestructura de información y telecomunicaciones ha crecido extraordinariamente, volviéndose compleja y difícil de gestionar. Cabría preguntarse qué conjunto de factores la hacen intrínsecamente vulnerable y si es posible tomar medidas estructurales para aumentar su resiliencia y sostenibilidad. En este artículo se intentará hacer un ejercicio de revisión de aquellos aspectos que provocan la fragilidad de nuestro patrimonio tecnológico y, por ende, la sociedad que estamos articulando. Repasando desde aspectos técnicos hasta las consideraciones sociales, se formularán algunas alternativas con el propósito de generar una reflexión sobre las mismas.

Abstract:

Cybersecurity is an issue that involves governments, private companies and citizens. The dependency that all social and economic sectors have on the information and communication infrastructure has increased extraordinarily and it is difficult and complex to manage. We wonder about the set of elements that make it inherently vulnerable, and if it is possible to make decisions that allow to increase its resilience and sustainability. In this paper, an effort is made to review such aspects that make weak our technology assets and, as a consequence, the society we have created around them. After the review of several technical and social issues, some alternatives are depicted with the aim to think about them.

Palabras clave:

Ciberseguridad, cloud, big data, ciberactivismo, BYOD, hacker, interconectividad, Internet.

Keywords: Cybersecurity, cloud, big data, cyberactivism, BYOD, hacking, interconnectivity, Internet.

INTRODUCCIÓN

La publicación en el año 2013 de la Estrategia de Ciberseguridad Nacional es una muestra más de que gobiernos y empresas son conscientes del problema que constituyen las agresiones a los sistemas de información de nuestro país. La ciberguerra es algo más que simples ataques, e implica el sabotaje y bloqueo de sistemas, el robo de propiedad intelectual y las actividades de inteligencia sobre personas y proyectos. De hecho, las entidades privadas consideran las intrusiones en sus sistemas de información como una de las cinco preocupaciones principales[1].

En respuesta a estas amenazas, se han creado diversas instituciones para velar por la seguridad: los distintos CERT, CNPIC, INTECO, COSDEF, ENISA, CCDCOE, etc. A su vez, ha habido un incremento en la regulación civil y penal sobre los delitos en la red, además de estándares y normativas de seguridad. Por otro lado, los ciberatacantes han evolucionado en sus objetivos, organización, sofisticación, complejidad y coordinación. Si el perfil de éstos era hasta hace bien poco el de hackers, ciberactivistas o redes más o menos organizadas de cibercriminales, ahora se les han sumado los cibercomandos de las fuerzas armadas de otros estados, cuyos objetivos son globales: militares, políticos y económicos.

En este marco, para un correcto planeamiento a largo plazo de una estrategia de ciberseguridad es necesario realizar un profundo análisis de las amenazas. Una precisa evaluación del riesgo necesita recopilar todas las posibles vulnerabilidades, estudiarlas tanto individualmente como relacionadas entre sí, y realizar un esfuerzo de imaginación para no limitarse a repetir los patrones del pasado[2] sino prever el futuro. En el momento de catalogar aquellos aspectos que están más expuestos a una ciberagresión, como en cualquier análisis de riesgos, podemos aceptar el *statu quo* actual y trabajar sobre él. Este enfoque es el predominante, y su resultado es una desproporción entre el esfuerzo necesario para la protección de los sistemas y los pocos medios que necesita el agresor para materializar una amenaza.

En el presente artículo, se pretende determinar cuáles son las raíces últimas de nuestras debilidades, revisando aquellos aspectos que podrían hacer intrínsecamente frágil nuestra infraestructura TIC y la sociedad que estamos articulando en torno a ella, para modificar la situación actual desde sus cimientos y conseguir un conjunto más racional y robusto. En

[1] A la altura de los problemas con Hacienda y los cambios legislativos según Lloyd´s Risk Index 2013. http://www.lloyds.com/~/media/Files/News%20and%20Insight/Risk%20Insight/Risk%20Index%202013/Report/Lloyds%20Risk%20Index%202013report100713.pdf

[2] Cita de Peter Drucker: El gran peligro de los momentos difíciles no son los problemas en sí mismos, sino actuar con los principios del pasado.

definitiva, buscar una estructura sostenible que aplique los principios de resiliencia establecidos en la estrategia española y europea sobre ciberseguridad[3].

LA VULNERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN

Una revisión de los incidentes de seguridad que se hicieron públicos durante el año 2013 resulta demoledora: se produjeron en las más importantes redes sociales, servicios de chat, dispositivos móviles, agencias aeroespaciales, sistemas gubernamentales civiles y militares de cualquier país, hospitales, universidades, centros financieros, de tarjetas de crédito, afectaron a millones de usuarios de todas clases, a datos personales, sensibles, contenidos de la comunicación, información secreta, al tráfico de internet, etc. Las causas fueron de todo tipo: negligencias, guerras comerciales, políticas, espionaje, mafias, gobiernos o simplemente gamberros. Por supuesto, no son conocidas las brechas no publicitadas; ni las actividades de la guerra cibernética; ni los miles de casos de acoso; ni los incidentes causados por fenómenos naturales, imprudencias o por la captura sistemática de datos a través de tecnologías como las cookies, etc. Las entidades en general, y las empresas en particular, constatan cómo cada año los incidentes de seguridad son más numerosos, más agresivos, con mayor impacto en sus activos o en los de los ciudadanos.

Debemos tener en cuenta que cualquier aplicación informática, ya sea de gestión, control, vigilancia o comunicaciones[4], tiene cientos de variables. El conjunto de relaciones entre ellas es de orden exponencial, y el número de situaciones del mundo real a las que han de enfrentarse es ilimitado[5]. Los cambios evolutivos de las aplicaciones[6,] y la reutilización de código y librerías[7] arrastran la herencia de especificaciones que implican conexiones, relaciones y funcionalidades no documentadas u obsoletas. Esto se manifiesta en una creciente complejidad de los sistemas TIC que imposibilita controlar todos sus aspectos y, por lo tanto, los hace intrínsecamente frágiles.

---

[3] Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro Bruselas, 7.2.2013 JOIN(2013) 1 final

[4] Incluso, a pesar de las férreas metodologías y la gran inversión en pruebas en el desarrollo de software aeroespacial, los sistemas siguen fallando, como en el siguiente caso: Airbus crash due to a software error http://www.youtube.com/watch?v=2eQpUgHkBcg

[5] Otro ejemplo de fallo de software que da al traste con una misión crítica, a pesar de que el entorno es de la misma criticidad que en la nota al pie anterior. DOUGLAS, Istbel. Et al. Mars Climate Orbiter failure board releases report, numerous NASA actions underway in response. JPL. 10 de noviembre de 1999. http://mars.jpl.nasa.gov/msp98/news/mco991110.html

[6] Sin firma. Computer Problem Disrupts Airline Reservation System. NewsOK. 18 de mayo de 1989 http://newsok.com/computer-problem-disrupts-airline-reservation-system/article/2266496

[7] LIONS, J.L. Informe de la Agencia Espacial Europea del accidente del vuelo 501 de ariane-5. ESA 19 de julio de 1996. http://www.upv.es/satelite/trabajos/pract_9/kike/paginas/accid.htm

La política que se está utilizando para hacer frente a esta situación es en su mayor parte reactiva. Es una huida hacia adelante con la inclusión constante de actualizaciones o parches. Esta forma de actuación supone un riesgo adicional[8], ya que implica la modificación de la aplicación a través de la red por parte de un tercero[9]. Además, el cambio de cualquier pieza de código supone la alteración de las relaciones entre los elementos de la aplicación y de dicha aplicación con otro software del sistema.

La experiencia demuestra que sólo es cuestión de tiempo que se produzca un incidente de seguridad en cualquier sistema de información; y que, además, este tendrá lugar de la forma más insospechada[10]. Es necesario asumir esta realidad y ser conscientes de que, a pesar de los esfuerzos, algún elemento estará siempre fuera de nuestro control. Hay que tener la modestia de admitir que puede haber siempre algo imprevisto, o que alguien ahí fuera tiene más imaginación que nosotros.

No sólo es necesario que la seguridad, en su sentido más amplio, aumente su peso como factor de diseño[11]. En la propia concepción de los sistemas se ha de aplicar el principio del fallo seguro: siendo conscientes de que el error se va a producir, es necesario tomar las medidas para que el impacto sea mínimo. Para implementarla, hay que realizar una gestión del riesgo más estricta que plantee escenarios en los que cada funcionalidad y cada elemento de información pueda ser comprometido, por muchas medidas de protección que se acumulen. De esta forma, tener preparados los planes de contingencia para dichas eventualidades y recortar la existencia de datos, conexiones, controles o procesos hasta dejar sólo los imprescindibles para la estricta funcionalidad del sistema.

[8] WILLIAMS, Martyn. Software glitch halts Tokyo Stock Exchange, Problem appears to have been caused by a software error related to a system upgrade. InfoWorld. 1 de noviembre de 2005. http://www.infoworld.com/d/developer-world/software-glitch-halts-tokyo-stock-exchange-910

[9] STORM, Darlene. Downloading of software updates for lifesaving medical devices proves very dangerous. ComputerWorld. 19 de junio de 2012. http://blogs.computerworld.com/malware-and-vulnerabilities/20554/software-updates-lifesaving-medical-devices-found-tainted-malware

[10] Un famoso ejemplo fue Key2Audio, el primer sistema anticopia de Sony. Este sistema significó una gran inversión y se presentó como inviolable, sin embargo, se rompía fácilmente escribiendo un raya con un rotulador sobre el propio CD. RAMOS, Alejandro. Hackeos memorables: Key2Audio, el primer sistema anticopia de Sony. Security by Default. 18 de mayo de 2010. http://www.securitybydefault.com/2010/05/hackeos-memorables-key2audio-el-primer.html

[11] CANDAU ROMERO, Javier, líneas de acción de la estrategia nacional de ciberseguridad, Cuadernos de estrategia 149, Secretaría General Técnica, Ministerio de Defensa, 2010. Disponible en: http://www.ieee.es/documentos/cuadernos-de-estrategia/detalle/Cuaderno_149.html

INTERCONEXIÓN E INTEROPERABILIDAD

En un análisis realizado entre responsables de sistemas de control de infraestructuras críticas[12], se destacaba que los ciberataques a los sistemas SCADA a través de la red son cada vez más frecuentes y sofisticados. El estudio concluía que el aspecto más preocupante era la certeza que detrás de muchos de ellos están implicados gobiernos extranjeros. Entre esos gobiernos no sólo está China[13], a la que se le atribuyen gran parte de los casos de ciberagresión, sino otros países, en particular Estados Unidos[14].

La mayoría de los ataques a los sistemas SCADA se producen a través de Internet porque gran parte de ellos están conectados directamente a algún tipo de red IP. La razón de esta conectividad la podemos encontrar en la cultura del "todo conectado" y de la gestión remota, que conlleva un ahorro en costes de administración, principalmente en el capítulo de personal especializado. Naturalmente, este grado de conectividad implica la necesidad de implementar elementos adicionales de seguridad al diseño básico de los protocolos de Internet, un diseño de los años 70 y 80, y que no estaba pensado para las aplicaciones actuales como comercio electrónico, móviles o ADSL en cada casa. Los niveles de protección añadidos (por ejemplo firewalls, capas cifradas, sistemas de monitorización de intrusos y más software de seguridad) han de adaptarse a ese diseño y también son susceptibles de sufrir incidentes. Según algunos estudios, a pesar de toda esa infraestructura de seguridad, las intrusiones avanzadas en los sistemas SCADA tardan una media de 476 días en ser detectadas[15].

Otro porcentaje importante de los ataques a los sistemas de control se produce por la conexión de equipos incontrolados directamente a un elemento interno, saltándose las barreras de seguridad. Este fue uno de los medios utilizados para la propagación de Stuxnet[16] (está ligado a la cultura BYOD), y es un problema que aparece no sólo en los

[12] BAKER, Stewart. Et al. En el punto de mira: las infraestructuras críticas en la era de la ciberguerra McAffee. 2010. http://img.en25.com/Web/McAfee/CIP_report_final_es_fnl_lores.pdf

[13] LEJARZA ILLARO, Eguskiñe. Estados Unidos - China: Equilibrio de poder en la nueva ciberguerra fría. IEEE, Documento de Opinión 60/2013. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO60-2013_Ciberguerra_Fria_EEUU-China_E.Lejarza.pdf

[14] En los años 80 el gobierno norteamericano inició la ciberguerra, dejándose "robar" a través de Canadá software necesario para la gestión del gaseoducto soviético. Este software contenía un troyano que colapsó en un momento dado todo el sistema. No fue el único éxito en la ciberguerra de esa época.

[15] Sin firma. Mandiant Releases Annual Threat Report on Advanced Targeted Attacks. Mandiant. 6 de marzo de 2012. https://www.mandiant.com/news/release/mandiant-releases-annual-threat-report-on-advanced-targeted-attacks/

[16] KUSHNER, David. The Real Story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied

sistemas SCADA, sino también en los sistemas militares o redes de mando y control. Esta circunstancia se facilita enormemente gracias a la interoperabilidad de estos sistemas entre sí, y especialmente con los dispositivos civiles, ya que resulta mucho más barato utilizar COTS y SOTS que desarrollar sistemas dedicados. Los interfaces son directos entre los dispositivos domésticos y los sistemas industriales y militares, lo que posibilita la comunicación con ellos y utilización de las mismas herramientas de intrusión.

El aumento en la conectividad de cualquier tipo de dispositivo está provocando cada vez más incidentes de seguridad, a cambio de una serie de ventajas a corto plazo. Es necesario implementar políticas más restrictivas de conectividad a la red, realizando un análisis crítico de los problemas a la seguridad que se originan a largo plazo y buscando alternativas a las estrategias de gestión remota. En cuanto a la interoperabilidad de sistemas, hay una corriente de opinión entre los especialistas del sector industrial que opina que parte de los problemas de seguridad podrían evitarse volviendo a utilizar sistemas y protocolos dedicados[17].

La conexión a la red de los sistemas de control no es un problema sólo de los sistemas industriales. Se está extendiendo a los hogares en lo que se ha venido a llamar Internet de las Cosas. Indudablemente, no tiene el mismo efecto paralizar un electrodoméstico que una central nuclear, pero una casa informatizada proporciona mucha información sobre los hábitos y forma de vida de sus habitantes, con el impacto que puede tener en la obtención de inteligencia. Por ejemplo, recientemente se han descubierto vulnerabilidades en las televisiones inteligentes que permiten espiar con imagen y sonido a sus usuarios[18].

Esta reflexión sobre la conectividad se podría extrapolar a los servicios de e-Goverment. En ese caso no hay elementos de control, pero sí la posibilidad de acceder a grandes volúmenes de información o a datos sensibles de particulares. Las administraciones públicas se lanzaron a la implementación de sus sedes electrónicas por ley, con plazos de puesta en marcha fijados por norma[19], y ya disponen por vía telemática de un 96% de sus trámites; aunque sólo un 5% de la población utiliza certificados para autenticarse[20]. Desde Europa se

---

Iran's nuclear-fuel enrichment program.. IEEE Spectrum. 26 de febrero de 2013 http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[17] NUTH, Thomas. SCADA Cyber Security: An International Issue. Tofino Security. 18 de abril 2013. http://www.tofinosecurity.com/blog/scada-cyber-security-international-issue

[18] Además de posibilitar otros ataques como acceder a las credenciales del usuario, el historial de búsqueda, cache, cookies, la contraseñas WIFI, etc. ROTHMAN, Wilson. Et al. Who's watching whom? Camera-equipped TV can be hacked, says researcher and Gary Merson NBC News 13 de diciembre de 2012. http://www.nbcnews.com/technology/whos-watching-whom-camera-equipped-tv-can-be-hacked-says-1C7596675

[19] Ley 11/2007, de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos

[20] Sin firma. ¿Por qué en España no aprovechamos los beneficios del DNI electrónico? Logisman 7 de agosto de 2013. http://custodia-documental.com/por-que-en-espana-no-aprovechamos-los-beneficios-del-dni-

ha impulsado esta política para volcar servicios administrativos a la red, aunque para ello haya que relajar las garantías de seguridad[21], y todo ello a pesar de los antecedentes producidos en Estonia[22].

RECOGIDA MASIVA DE DATOS

La mayor parte de los incidentes de seguridad tienen como consecuencia el robo de gran cantidad de datos de usuarios y, casi siempre, los sistemas están dotados de medidas de protección (claves de acceso, comunicaciones cifradas, etc.); incluso empresas con certificados de seguridad[23]. Enlazando con lo comentado en el último apartado anterior, es un hecho que en muchos servicios se recogen más datos de los necesarios. Se conservan más allá de su ciclo de vida y se mantienen accesibles a través de la red sin una utilidad inmediata. La implementación de políticas de recogida masiva de información implica que, a la hora de materializarse una amenaza, el impacto sobre la confidencialidad será mayor. Indudablemente, la información es un activo de gran valor, por lo que añadir o conservar datos que no sean realmente necesarios para los procesos de negocio alentará el interés de los posibles atacantes.

Tener información en un sistema lo hace vulnerable en su confidencialidad, integridad o disponibilidad. Esa probabilidad aumenta cuando el sistema está conectado a una red, y se dispara cuando esa red es accesible de algún modo a través de redes públicas como Internet. En el caso de ciberataques, los recursos que se podrán emplear para superar las medidas de seguridad guardarán relación con el valor (para el atacante) de lo que dichas medidas protegen.

La recogida de datos que no tienen una utilidad futura, ni siquiera a corto plazo, constituye una amenaza en sí misma para la entidad que los almacena; ya sea un servicio de inteligencia o una empresa privada. Si es un activo del que no se está sacando un rendimiento inmediato, será explotado por terceros de alguna forma, ya sea debido a filtraciones, utilización política o robo. Y la experiencia nos dicta que esto sucederá, antes o después.

---

electronico/

[21] Por ley se relaja la definición de lo que es una firma electrónica. Ley 11/2007. Artículo 16 Utilización de otros sistemas de firma electrónica.

[22] TIKK Eneken, et al. International Cyber Incidents, Legal Considerations. CCDCOE Estonia, 2010 http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

[23] EFE, Protección de datos abre una investigación por el robo de datos en el INTECO, El Mundo, 7 de julio de 2011

Hay que dar un paso atrás en las políticas de recogida masiva de información, y estas políticas han de imponerse tanto a empresas públicas como privadas, en especial en las compañías de servicios en Internet. Cada dato recogido ha de estar plenamente justificado, y su conservación más aún. Además, debe someterse a una revisión restrictiva el conjunto de información accesible a través de la red retirando tanta información como sea posible. Esa revisión ha de realizarse desde el prisma de que existe siempre una posibilidad de que la información sea comprometida, y de las implicaciones de que se materialice una amenaza.

LA BASE INDUSTRIAL

No todas las ciberamenazas se presentan como intrusiones técnicas. Hay otros factores que pueden afectar a la disponibilidad de nuestro patrimonio tecnológico. Por ejemplo, durante dos años consecutivos se produjeron catástrofes naturales, la primera en Taiwan, un terremoto en 2010, y luego en Japón, el famoso tsunami de 2011. En el primero no hubo víctimas y en el segundo, si atendemos fríamente a los porcentajes, afectó de forma mínima al conjunto de la población[24]. En cambio, sí tuvieron un impacto importante en el suministro de componentes electrónicos para la producción industrial de multitud de productos: desde ordenadores hasta coches[25].

En la zona de Corea-Japón-Taiwan-China se concentra gran parte de la producción de componentes básicos para la industria electrónica. Aunque las cifras de beneficios otorgan sólo un 50% del mercado al tándem China-Japón[26], el 21% correspondiente a Europa se basa en productos de valor añadido, no en componentes básicos, es más: la tendencia es que esta distinción, esta relación de dependencia, crecen cada año a ritmo constante[27] especialmente en beneficio de China.

El área de extremo oriente está amenazada tanto por desastres naturales como por inestabilidades políticas, principalmente procedentes de Corea del Norte, la rivalidad entre Japón, China y Taiwán por las islas Senkaku y la ciberguerra encubierta entre China y EEUU. Estas tensiones se han materializado a veces en embargos económicos. Pensar que el inmenso beneficio económico que suponen esos mercados impedirá una crisis podría ser un

[24] Hubo un 0,008% de víctimas sobre el total de la población.
[25] En el caso de Taiwan: http://www.electronicsweekly.com/news/components/led-lighting/lcd-shortages-may-follow-earthquake-in-taiwan-2010-03/. Y en el caso de Japón: http://news.techeye.net/business/tablet-chip-and-car-component-shortages-continue-post-quake
[26] http://www.businessvibes.com/blog/industry-insight-electronic-industry-eu
[27] http://www.semiconductorintelligence.com/?p=860

error[28]. Más aun teniendo en cuenta la falta de sostenibilidad de la economía y la política chinas, y que los ciclos económicos parecen cumplirse con matemática precisión[29].

Aunque nos encontramos en un mercado globalizado, la deslocalización ha originado un efecto de centralización de los suministros en determinados puntos del planeta, en vez de una redistribución homogénea. Esta estrategia es fuente de grandes beneficios económicos, pero será el origen de inestabilidades a largo plazo, similar a lo ocurrido en la crisis del petróleo del 73. Como sucedió en aquel caso, es necesario plantearse dicho escenario de crisis y prever alternativas a las fuentes de suministro, de componentes elementales y de sistemas. Es importante impulsar la base industrial, que trasciende la específica para la defensa, sino que se extiende a la que soporta nuestras infraestructuras críticas y nuestro tejido comercial. Esa base industrial ha de gestionarse localmente, para garantizar su control y disponibilidad, y así disminuir nuestro grado de dependencia.

PATRIMONIO TECNOLÓGICO Y CABALLOS DE TROYA

En 1974, los británicos desvelaron cuál era el secreto de la fuente de información ULTRA, utilizada durante la II Guerra Mundial. Resultó ser la capacidad de sus servicios de inteligencia para romper el cifrado de la máquina Enigma. Para muchos países de la Commonwealth fue una sorpresa desagradable, ya que los ingleses les habían distribuido durante veinte años las máquinas capturadas a los alemanes para que las empleasen como un medio de cifrado seguro[30].

Los sistemas de cifrados siempre han estado bajo el estricto control de los servicios de inteligencia de los respectivos países[31], lo que siempre ha generado incertidumbres sobre la fiabilidad de los mismos[32]. La posible existencia de "puertas traseras" en las aplicaciones afecta no sólo a los sistemas de cifrado, sino a todos los elementos que forman parte de nuestro patrimonio tecnológico: infraestructura de comunicaciones, protocolos de datos, sistemas operativos, aplicaciones, etc. La utilización sistemática de elementos que son "cajas

[28] Una previsión similar se realizó justo antes de la Gran Guerra, cuando los analistas auguraron que un conflicto europeo no podría prolongarse más de seis meses por el daño a los mercados financieros
[29] La crisis de los 80' en EEUU. De los 90 en Japón, 2000 Corea, 2010 Unión Europea.
[30] SINGH, Simon. The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography. Doubleday Books, 1999
[31] En particular para su exportación: EAR Controls for Items That Use Encryption http://www.bis.doc.gov/index.php/policy-guidance/encryption
[32] En 1997, se hizo público que los algoritmos de clave asimétrica se desarrollaron en secreto por James H. Ellis, Clifford Cocks y Malcolm Williamson en las Sede de Comunicaciones del Gobierno Británico en 1973. Existen dudas sobre la elección de las S-box de DES, de la modificación en el algoritmo AES con claves de 192 bits o su limitación a bloques de 4 bytes, la negociación del cifrado en el protocolo Https, etc

negras", sistemas o infraestructuras gestionadas incluso por empresas extranjeras, abre la posibilidad de que terceros puedan controlar los sistemas críticos en un momento de crisis, y también permite la obtención de inteligencia suficiente (usuarios, claves, perfiles, etc.) para su utilización en otro tipo de ataques más avanzados o a más largo plazo.

Los países que pueden aprovecharse de la introducción de "caballos de Troya" son aquellos que tienen una posición de supremacía en la industria tecnológica[33]. Para contrarrestar esta situación se ha creado un marco de certificación de seguridad de productos y sistemas[34], la acreditación de laboratorios públicos y privados, y la participación en acuerdos para el reconocimiento e intercambio de acreditaciones con otros países basadas en la utilización de estándares[35].

Fundamentar la ciberseguridad en la colaboración y la buena voluntad de nuestros aliados puede resultar muy arriesgado, como se ha visto en el caso PRISM[36], pues su política se va a adaptar a los principios de Palmerston[37]. Utilizar tecnología desarrollada por terceros países supone exponerse a que puedan existir agujeros introducidos de forma deliberada, debilidades que podrían ser explotadas en caso de conflicto o introducidas en las actualizaciones periódicas. En el mejor de los casos, supone utilizar unas técnicas que están un paso por detrás de las empleadas por el país proveedor.

Para tener realmente el control del patrimonio tecnológico es necesario algo más que incrementar la capacitación técnica en ciberseguridad. Es fundamental conservar nuestras propias patentes, crear nuestro propio conocimiento e impulsar nuestra propia industria. No se puede construir una capa de seguridad efectiva sobre un conjunto de elementos no confiables. Si parte de ese patrimonio lo forma la infraestructura de comunicaciones, también Su tecnología y gestión y propiedad no puede dejarse, sin ninguna supervisión, a la dirección de empresas de terceros países.

[33] Siempre hay una sospecha de que China lo está llevando a cabo: WND - China: 'Pervasive access' to 80% of telecoms - Even military encryption can no longer guard sensitive data 07/01/2012 Michael Maloof http://www.wnd.com/2012/07/chinese-have-pervasive-access-to-80-of-worlds-telecoms/

[34] Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información

[35] CCRA - Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security

[36] SANCHEZ, Rosalía. Berlín no cree al 'amigo americano'. El Mundo 17 de enero de 2014 http://www.elmundo.es/internacional/2014/01/17/52d9909422601d23258b457e.html

[37] Lord Palmerston: "Inglaterra no tiene amigos permanentes ni enemigos permanentes. Inglaterra tiene intereses permanentes"

EXTERNALIZACIÓN: LOS SERVICIOS EN LA NUBE

El 19 de enero de 2012, el FBI cerraba por sorpresa los servicios de Megaupload, un proveedor de servicios en la Nube. Esta acción causó pérdidas económicas a PYMES y autónomos españoles en una forma difícil de evaluar[38]. En dicha intervención no se tuvieron en cuenta ni los derechos ni los intereses de dichas empresas[39].

Que el FBI fuera el que realizase las actuaciones, y por muy justificados que fuesen sus motivos, no obstaba los perjuicios para nuestras empresas, resultando un ataque a la disponibilidad y confidencialidad de sus datos. Este incidente en la Nube no es un hecho aislado, sino uno de los muchos en los que la seguridad en ese entorno se ha comprometido, gravemente además[40]. Algunos estudios estiman que la pérdida por la caída de servicios de Cloud ha tenido un impacto de más de 50 millones de euros desde 2007[41].

Las soluciones de Cloud, del tipo Nubes Públicas de grandes proveedores de Internet, suponen basar en servicios física y fiscalmente fuera de España parte de nuestros datos y procesos. El empleo masivo de soluciones Cloud supone, además de la externalización señalada, dar un paso más en nuestra dependencia respecto a las redes de comunicaciones necesarias para el acceso a la información. Como colofón, implica desmantelar el patrimonio tecnológico y sobre todo el capital humano: personal con el *know-how* del negocio y los procesos técnicos. Esta infraestructura, en caso de necesidad, será muy difícil de recuperar[42].

El concepto de Cloud supone la concentración en unos pocos puntos singulares de gran parte de los procesos que realizan entidades españolas, lo que facilita (y hace más rentable) la acción de un potencial atacante, quien no tendría que atender a infinidad de objetivos,

---

[38] de Juana R. *Qué implica el cierre de Megaupload para las pymes*. 7 de febrero de 2012 http://www.muypymes.com/2012/02/07/que-implica-el-cierre-de-megaupload-para-las-pymes

[39] Sanz J. *EEUU ignora al Gobierno de España en relación a la posible recuperación de ficheros de Megaupload*, 19 de marzo 2012, http://www.adslzone.net/article8200-eeuu-ignora-al-gobierno-de-espana-en-relacion-a-la-posible-recuperacion-de-ficheros-de-megaupload.html

[40] Mah P. *Dropbox's multiple security problems*, 19 de agosto de 2011 By http://www.fiercecio.com/techwatch/story/dropboxs-multiple-security-problems/2011-08-19. Otro caso: *Epsilon Breach Deals Another Blow to Cloud Security*, 8 de abril de 2011 http://www.infosecisland.com/blogview/12814-Epsilon-Breach-Deals-Another-Blow-to-Cloud-Security.html

[41] Essers L. *Cloud downtime has cost more than £45 million since 2007* IDG News Service 12 de junio de 2012 http://www.computerworlduk.com/news/cloud-computing/3364982/cloud-downtime-has-cost-more-than-45-million-since-2007/?intcmp=in_article;related

[42] Este análisis se realizó en el caso de la migración de los servicios de la ciudad de Los Ángeles al servicio de cloud, concluyéndose que: "si la Ciudad decide utilizar estos servicios…. será prohibitivo en coste volver a la actual estructura gestionada por la propia Ciudad". Jansen W. *Guidelines on security and privacy in public cloud computing.* NIST National Institute of Standards and Technology, diciembre 2011

sino que podría alcanzar gran efectividad focalizando sus actuaciones sobre un puñado de proveedores. La materialización de una amenaza sobre un servidor de Cloud se convierte en una brecha que afecta a un conjunto significativo de empresas o entidades de forma simultánea. Estas amenazas podrían ser ataques sobre los servicios de Cloud que afecten a la confidencialidad, caídas de servicio por problemas técnico-comerciales[43] en la propia Nube o en la red, accesos indebidos a la información por los propios proveedores o intervención de datos y servicios por las autoridades nacionales donde residen los servidores o están registradas las empresas[44]. En cuanto a este último aspecto, debemos recordar que antes del escándalo PRISM, o la iniciativa CISPA, el FBI ya manifestaba sus intenciones de controlar en tiempo real aplicaciones en la Nube como Gmail o Dropbox[45]. Estos programas de control también se han destapado en Reino Unido, la India y otros países[46].

En relación a la posible intervención de agentes estatales en la vulneración de la confidencialidad de los datos, es necesario tener en cuenta tanto el contenido de la comunicación como la metainformación asociada al contenido, en su mayor parte información de tráfico: localización geográfica de los comunicantes; su identidad; red de relaciones; información sobre los dispositivos conectados; volumen de información transmitida por un usuario; volumen de tráfico de la entidad, estadística y puntualmente, etc. Esta metainformación es aún más interesante cuando se toma en consideración la Nube móvil[47].

La tecnología de Cloud tiene grandes ventajas, que han de ser aprovechadas siempre con ciertas limitaciones, y teniendo presente la criticidad de los datos o servicios[48]. No se debe fundamentar la decisión de la migración a la Nube basándose únicamente en el ahorro de costes a corto plazo, o como una salida fácil en época de crisis. En el caso de la industria de defensa se han planteado otras consideraciones, como por ejemplo el caso de la empresa

[43] Un aumento unilateral del coste de los servicios, una modificación/suspensión de las condiciones de prestación, un cambio de estrategia empresarial, por absorciones, por el cierre de la compañía o por situaciones de crisis

[44] Incluso más allá, ya que el FBI en el caso Megaupload intervino una empresa domiciliada en Hong-Kong

[45] Sin Firma. El FBI busca controlar toda comunicación en la 'nube' a tiempo real, como Gmail o Dropbox. El Mundo. 27 de marzo de 2013 www.elmundo.es/elmundo/2013/03/27/navegante/1364368758.html

[46]GUTIERREZ, Juan Carlos. India lanza su sistema de vigilancia nacional para controlar internet, llamadas y mensajes. Compunoticias. 9 de mayo de 2013. http://compunoticias.com/2013/05/09/india-lanza-su-sistema-de-vigilancia-nacional-para-controlar-internet-llamadas-y-mensajes/

[47] Un ejemplo de esto ocurre con las redes sociales: ENGLAND, Jason. We Know Your House' Shows How Many People Reveal Their Home Address On Twitter. New Rising Media. 14 de agosto de 2012 http://newrisingmedia.com/all/2012/8/14/we-know-your-house-shows-how-many-people-reveal-their-home-a.html

[48] Por ejemplo, se ha implementado la gestión de la Unidad de Arbolado Urbano del Ayuntamiento de Madrid sobre Windows Azure, lo que parece un correcto balance entre el tipo de servicio y el beneficio económico.

BAE Systems, que abandonó sus planes de despliegue de aplicaciones[49] sobre Microsoft 365 por no tener una garantía de confidencialidad frente a sus competidores norteamericanos. En este punto, sería importante tener en cuenta las ventajas de las Nubes Privadas[50] para la Administración Pública, frente a los riesgos que plantea el uso de oligopolios de Cloud no sometidos a la regulación nacional (una iniciativa ya se ha planteado en Suecia[51] y Alemania[52]) y proponer alternativas, como seleccionar a aquellos proveedores de Cloud públicos que estén localizados físicamente en España. En cualquier caso, contratar servicios de Cloud en ningún caso puede suponer una delegación de las obligaciones de gobernanza de los sistemas de información y de las responsabilidades que de ellas se derivan.

MODAS Y TENDENCIAS TECNOLÓGICAS: BRING YOUR OWN DEVICE

Durante la guerra de Irak, un ataque relámpago con morteros destruyó cuatro helicópteros Apache recién llegados a una base norteamericana. La precisión del bombardeo fue posible porque los soldados tenían la costumbre de tomar fotos, usando sus teléfonos móviles, de la llegada de cada nueva flota y, por supuesto, subir dichas fotos a Internet. Las imágenes incluían metadatos, en particular datos GPS, que permitían localizar con total exactitud la posición de las aeronaves[53].

BYOD define una práctica en la que el dispositivo personal, (*smartphone*, *tablet* o portátil) acompaña al usuario cuando se desplaza a su centro laboral. En algunos casos, se confunde con el propio dispositivo de trabajo. Incorpora no sólo el tratamiento de datos (memoria, imagen, sonido, localización, etc.), sino también servicios de comunicaciones independientes. Los canales de distribución de información ya no son únicamente los corporativos. Se añaden canales alternativos como Whatsapp, Skype, Line, además de la utilización de Nubes personales. Estas últimas son un agujero de seguridad que posibilita la

[49] MANDALIA, Ravi. BAE Systems Abandons Microsoft Cloud Plans Citing Patriot Act. IT Proportal 8 de diciembre de 2011 http://www.itproportal.com/2011/12/08/bae-systems-abandons-microsoft-cloud-plans-citing-patriot-act/

[50] Una Nube Privada no significa que el proveedor sea una empresa privada, sino que le proveedor es la misma entidad, o una subcontrata particular para implementar de forma exclusiva sus servicios. Además, siempre hay excepciones en función del tipo de información que se trate, como es el caso de la gestión de la Unidad de Arbolado Urbano del Ayuntamiento de Madrid que se ha implementado sobre una nube de Windows.

[51] WAUTERS, Robin. The Next Web: Dark clouds loom over Google in the EU as Swedish data regulator kills a Google Apps deal. The Next Web. 14 de junio de 2013 http://thenextweb.com/google/2013/06/14/sweden-google-data-protection/

[52] Sin Firma. Cloud threatened: German DPAs stop granting permission for data transfers to non-EU countries Privacy Laws & Business. 8 de agosto de 2013 http://www.privacylaws.co.uk/Publications/enews/International-E-news/

[53] RODEWIG, Cheryl. Geotagging poses security risks. WWW.ARMY.MIL 7 de marzo de 2012 http://www.army.mil/article/75165/Geotagging_poses_security_risks/

existencia de puentes con los sistemas de la empresa cuando, desde el dispositivo corporativo, el usuario accede a las dos Nubes de forma simultánea, la profesional y la personal. Existen datos que sitúan en el 60% las empresas que han tenido algún problema serio debido al uso de dispositivos personales conectados a la red corporativa con una inadecuada política de seguridad[54].

Para algunas empresas, la política BYOD tiene ciertas ventajas, sobre todo en aquellas con pocas infraestructuras, en las que se prima la movilidad geográfica y laboral. Esta tendencia es impulsada también por los propios empleados; bien porque se sienten más confortables al manejar su entorno doméstico, bien porque están en entidades con pocos recursos para dotar a sus empleados de dispositivos de calidad para realizar su trabajo. La situación ha llegado a tal punto que, en 2012, se estimaba que el 96% de las empresas permitía estas actuaciones y que la media de dispositivos por empleado alcanzaba 2,8 equipos[55].

Estos dispositivos no están bajo el control de la política de seguridad de la empresa. Los sistemas son administrados por los propios usuarios que no incorporarán medidas que dificulten su trabajo, les imponga protocolos tediosos o limiten las posibilidades de sus dispositivos. Los usuarios estarán deseosos de tener la libertad de compaginar su actividad laboral con la privada. En muchos casos, esos usuarios tendrán responsabilidades en más de una entidad, de forma directamente ejecutiva, o de asesoría, consultoría, formación o cualquier otra.

Los riesgos inherentes a la práctica BYOD van más allá de una acción directa por parte de un ciberagresor. Esta práctica permite el seguimiento del individuo incluso dentro de las dependencias de la propia empresa, con determinación de dónde y con quién se reúne, permite filtraciones de información entre las actividades personales y profesionales de la empresa, introducción de virus, desestabilización en caso de ataques utilizando técnicas de ingeniería social, etc.

Algunas entidades ya se han planteado limitar el uso indiscriminado de dispositivos personales[56], mientras otras buscan evitar su utilización combinada con las Nubes personales. Para hacer frente a estas amenazas, hay que contemplar esta situación en el marco de la política de seguridad de la empresa, no como una moda tecnológica, sino

[54] SARO LUNA, Javier. Et al. La gestión segura de la información e movilidad ante el fenómeno BYOD: ¿Bring your own device = Bring your own disaster? Revista de seguridad en informática y comunicaciones, abril 2013 pg-65-73

[55] Sin firma. Los responsables TIC respaldan el fenómeno BYOD. Cisco. 16 de mayo de 2012 http://www.cisco.com/web/ES/about/press/2012/2012-05-16-cisco-los-responsables-de-ti-respaldan-el-fenomeno-byod.html

[56] SAVVAS A. Most firms block BYOS in the cloud, Computerworld UK, 17 de julio de 2012 http://www.computerworlduk.com/news/cloud-computing/3370488/most-firms-block-byos-in-cloud/

gestionando el riesgo que suponen e incluyendo los mecanismos para limitar el impacto de su uso incontrolado.

En definitiva, BYOD es sólo un ejemplo de los efectos colaterales de la adhesión a tendencias tecnológicas impulsadas por intereses comerciales a corto plazo. De forma continua aparecen nuevas aplicaciones y dispositivos, como gafas de realidad aumentada, chips implantados[57], drones de empresas particulares o cualquier otro; tendrán, a buen seguro, efectos colaterales insospechados. No podemos permitir que sólo las leyes del mercado modelen nuestra sociedad, al contrario; es necesario mantener una supervisión constante y realizar un análisis crítico de cada innovación. Con independencia de las campañas de marketing, hay que normalizar e imponer límites utilizando tanto una visión estratégica de ciberseguridad como la protección de los derechos de los ciudadanos[58].

BIG DATA Y LOS OLIGOPOLIOS DE INFORMACIÓN

Desde la década de los noventa, se han ido utilizando los términos "Data Mining", “Knowledge Discovery in Databases”, "Information Fusion" o, más recientemente, "Data Science" para referirse a las técnicas que generan información a partir de relacionar, estructurar, cruzar, comparar, o proyectar datos en entornos multidimensionales. Actualmente se emplea el término Big Data, un derivado de los términos anteriores, para describir la explotación de las bases de datos corporativas y con gran volumen de información, complementadas con datos de terceras fuentes.

En el sector de Internet han surgido grandes oligopolios que ofrecen servicios a nivel global, incluyendo en un único paquete buscador, mensajería, compras, relaciones personales, almacenamiento, geolocalización, detección del fraude, marketing, salud, aplicaciones profesionales y de ocio, etc. Internet encarna el principio de Heisenberg, consistente en que no puedes observar sin modificar la realidad, lo que en este caso implica que cada acceso a la red deja un rastro que alimentará el conjunto de datos de la misma red. Por lo tanto, este puñado de entidades acumula información de sus usuarios en múltiples facetas de su vida. Gracias a su abanico de productos, pueden relacionar estos datos con información geográfica, datos de telecomunicaciones, de cámaras, de sensores, incluso de los electrodomésticos[59].

[57] EUROPA PRESS. Una discoteca catalana implantará un chip bajo la piel a personajes famosos. El Mundo 17 de marzo de 2004 http://www.elmundo.es/navegante/2004/03/17/esociedad/1079536632.html
[58] Desde esta última óptica, ya se ha puesto freno a iniciativas como Digital Signage, etiquetado de prendas con RFID, el scoring automático, la utilización de cookies, etc.
[59] DANS, Enrique. El año de Internet de las Cosas: Google compra Nest. Blog. 14 de enero de 2014.

De esta forma surge el concepto de 'Big Data', pero en un sentido más amplio, como el tratamiento de datos a una escala desconocida hasta ahora en número de personas involucradas y en diversidad de los tratamientos[60]. La información puede ser retenida durante largos periodos de tiempo[61] y puede ser analizada exhaustivamente para cruzar, comprender y aprovechar todo el valor de los datos en relación a ese individuo, sus relaciones, sus patrones de conducta, su proceso de toma de decisiones, su psicología, su evolución, su catalogación dentro de grupos y la elaboración de tendencias dentro de dichos grupos.

El impacto económico del Big Data es enorme. De hecho, ya se está empleando en el marketing y la prospección comercial de forma general (planificación de campañas publicitarias, localización de centros comerciales, distribución de productos) y para el *targeting* y *scoring* individualizado en función del perfil de cada cliente, un perfil muy detallado.

La información que tienen esas corporaciones sobre individuos específicos o sobre segmentos de población es lo suficientemente buena como para emplearla más allá que en inteligencia económica. Estas empresas se han convertido en grandes corporaciones en el sector de las tecnologías y la influencia que podrían ejercer por sí mismas, o empujados por los gobiernos de sus países de origen o los grupos de interés que los soportan, es enorme. Su existencia compromete el propósito original de las iniciativas como Open Data, el libre acceso a las bases de datos en manos de las administraciones públicas, o de las leyes de transparencia. Los grandes grupos del sector de la información son los que tendrán más recursos para la explotación y el cruce de esta información procedente de la Administración.

Entidades como las descritas constituyen un riesgo en sí mismas: pueden facilitar la existencia de grandes programas de vigilancia electrónica, y están sujetas a posibles fallos de seguridad que comprometan toda esa información[62]. Hay que plantearse si los monopolios actuales son beneficiosos para nuestro país, y para el conjunto de Internet, y hasta qué punto condicionan el ejercicio de las libertades de los ciudadanos. La división de estas grandes corporaciones, tanto de forma horizontal, territorial o por servicios, es una opción a plantearse. Tuvo un antecedente en el caso AT&T en los años setenta[63] cuando el gobierno

---

http://www.enriquedans.com/2014/01/el-ano-de-la-internet-de-las-cosas-google-compra-nest.html

[60] Opinion 03/2013 on purpose limitation. Article 29 Data Protection Working Party: idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf

[61] Ni siquiera es necesario tener todos los datos almacenados durante todo el tiempo, sino sólo el resultado del análisis de los más antiguos.

[62] KORNER, Anthony W. Google buys Nest just as Internet of Things suffers first global cyber Attack. Forbes. 18 de enero de 2014 http://www.forbes.com/sites/anthonykosner/2014/01/18/google-buys-nest-just-as-internet-of-things-suffers-first-global-cyber-attack/

[63] El proceso de división se culminó en los años 80 aunque se había iniciado en 1974 invocando la legislación

norteamericano consideró que la concentración era económicamente beneficiosa para la compañía, pero no para el conjunto del Estado.

LA SOCIEDAD DEPENDIENTE

A principios de 2013, una noticia increíble saltó a los medios de comunicación[64]: una mujer belga que trataba de alcanzar con su coche el norte de la ciudad de Bruselas realizaba por error un viaje de Bélgica a Zagreb, cruzando toda Europa, porque había estado siguiendo las indicaciones erróneas del navegador GPS de su vehículo. En vez de recorrer 150 kilómetros, terminó realizando un viaje de más de dos mil.

Probablemente esta historia no sea completamente cierta, pero sí ejemplifica el nivel de dependencia al que ha llegado nuestra sociedad respecto de la información proporcionada por sistemas digitales. Uno de los aspectos en los que más se enfatiza cuando se habla de ciberseguridad es lo importante que es la educación de los usuarios. Hay que destacar que parte de esa educación ha de estar dirigida a que estos eviten depender en exceso de las tecnologías de la información. Esto es más evidente en las nuevas generaciones, que han encontrado en la electrónica la solución a muchos de sus problemas de la vida diaria. Es una nueva cultura, una nueva forma de entender el entorno. Ya hay muchas personas que realmente dependen en su devenir profesional, personal e incluso afectivo de los servicios digitales, -especialmente online- conectados permanentemente a Internet.

Cuando se habla de la educación de usuarios, suele entenderse que el mensaje está dirigido a los consumidores, si bien debe tenerse también en cuenta a quienes toman decisiones estratégicas sobre los sistemas de información. En agosto de 2012, una empresa financiera perdió 440 millones de dólares en 45 minutos porque su sistema emitió de forma automática masivas órdenes de venta de acciones debido a un "error de software"[65]. Alguien había tomado la decisión de actuar sin intervención humana en determinadas condiciones. Este no es un caso aislado en el sector financiero. Existe una tendencia a delegar la toma de

anti-Trust. En ese momento AT&T controlaba prácticamente todas las comunicaciones locales y de larga distancia en USA, directorios telefónicos y suministro de sistemas de comunicaciones, su bucle local tenía incluso más cobre que el mayor productor mundial, Chile. En ese momento, a parte de las turbulencias políticas y económicas, AT&T fue objeto de ataques de phreakers (los antiguos piratas telefónicos) que causaron diversos apagones de la red telefónica y fueron duramente perseguidos por el FBI.

[64] GÓMEZ, J. La increíble historia de una mujer que se perdió usando el GPS y acabo en Croacia. Motor.es 15 de enero de 2013 http://www.motor.es/noticias/error-gps-la-increible-historia-de-una-mujer-se-pierdio-usando-el-gps-y-acabo-en-croacia-201312691.php

[65] PRATLEY, Nils. Knight Capital's computer 'glitch' shows dangers of desire for faster trading. Investors' and markets' demands for high-frequency trading ignores the need for the system to have a reliable circuit breaker. The Guardian, 6 de agosto de 2012 http://www.theguardian.com/business/nils-pratley-on-finance/2012/aug/06/knight-capital-computer-glitch-trading

decisiones a sistemas automáticos sin supervisión, decisiones que afectan a las personas. Es el caso de los sistemas de videovigilancia[66] y seguridad remota, o aquellos que evalúan la solvencia o confianza de un sujeto a través de Internet, con el peligro que las consecuencias de un error pueden acarrear en aspectos como la privacidad[67], la catalogación automática como "persona de riesgo" o directamente su manipulación malintencionada.

En los planos personal y profesional, utilizar de forma extensa sistemas digitales interconectados es algo positivo, eficiente, rápido; y, gracias a las economías de escala, barato. Pero esto se ha de compatibilizar con una educación de los usuarios para que no se conviertan en incapacitados si carecen de las ayudas online; para que estén preparados y sigan adelante ese día que no hay conexión en la oficina y dar esa misma educación a los gestores que basan decisiones críticas en sistemas automáticos sin supervisión humana. Es necesario mantener la capacidad de resiliencia de la sociedad para que, en caso de un hipotético apagón digital, como el planteado en el efecto 2000 o el provocado en Estonia, no se entre en un estado de parálisis con un sentimiento de vulnerabilidad; sino que la población se encuentre material y psicológicamente preparada para afrontar dicho reto.

EL ASPECTO SOCIAL DE LAS TIC

Las TIC, y las amenazas que se ciernen sobre las mismas, van mucho más allá de incidentes en el plano puramente técnico, abarcan también aspectos sociales. Las nuevas técnicas de comunicación y la fragilidad de su seguridad son el primer factor de riesgo. La Primavera Árabe, el caso PRISM, Anonymous y Wikileaks, entre muchos otros[68], han tenido más impacto que cualquier caso de ciberataque tecnificado. Algunos de estos hechos han cambiado nuestra concepción del mundo.

Ciberactivismo y ética hacker introducen un nuevo lenguaje, una forma alternativa de entender nuestras relaciones, con un novedoso estilo de activismo social. Bajo esta denominación se agrupan iniciativas con objetivos muy diversos: denuncia social, indignados, creadores de opinión, lobbies, grupos de presión, hackers éticos, piratas, filántropos, redes de financiación, terroristas, etc. Un gran abanico de opciones, a veces totalmente contrapuestas, en el que sus participantes pueden deslizarse de un extremo a otro.

[66] Existen sistemas que te catalogan de forma automática como sospechoso simplemente por tu actitud corporal, o que te evalúan como un cliente fiable a través de Internet por la configuración de tu ordenador.
[67] Como resultó de la recogida de datos de los navegadores Tom-Tom por parte de la policía de tráfico holandesa con propósitos sancionadores.
[68] Como las campañas: no les votes, canon, ley Sinde, manifiesto, no a la guerra, boicot a Tele5, etc.

El ciberactivismo tiene muchos aspectos positivos, como abrir nuevas vías de participación ciudadana y canales creativos a las asociaciones[69]. Por su parte, los hackers éticos desvelan los límites y problemas de los servicios en Internet; actúan de vigilantes evitando excesos y publicitan las vulnerabilidades. Sin ellos, viviríamos ignorando gran parte de los problemas que ahora debemos solucionar[70].

Sin embargo, el ciberactivismo o la actitud "hacker" se ha convertido en un concepto fácil de vender, divertido, que parece carente de riesgo y que se puede realizar desde el propio puesto de trabajo. El ciberactivismo es cómodo en relación al activismo, ya que la cultura de la adhesión es más sencilla y el nivel de compromiso se mediatiza y trivializa. Esto ha derivado hacia una atomización de las causas y a que se prendan grandes incendios con causas pequeñas.

Si no hay que demonizar la ética hacker, tampoco puede servir esta de justificación para cualquier actitud. Es difícil poner un límite y distinguir dónde termina la positiva movilización ciudadana y dónde empieza el acoso o la guerrilla ciberurbana. En caso contrario, es fácil que el propio ciberactivista sea utilizado por intereses más mezquinos, que, en el peor de los casos, serán parte de la maquinaria de una mafia. No hay que caer en la ingenuidad de la "Declaración de Independencia del Ciberespacio"[71]. Son los hackers de los años 80 los que ahora, a través de poderosas empresas que han creado, luchan contra sus sucesores protegiendo sus intereses comerciales[72]. Incluso las herramientas que están usando son en algunos casos desarrollos militares[73]. Los cibermovimientos, muchas veces, están más estructurados de lo que sus militantes pretenden. Como todo sistema asambleario, son muy manipulables. De ahí la aparición de nuevos personajes en la red como son los community managers, los troles[74] y el autotroleo para generar movimiento en la red.

Muchos no son conscientes de que la impunidad en la red está desapareciendo; de que la tipificación de delitos se ha ampliado; de que las acciones en Internet han de realizarse

[69] Como la exitosa campaña de Greenpeace contra Nestlé en youtube: http://www.youtube.com/watch?v=QV1t-MvnCrA

[70] OLSON, Parmy. SIM Cards Have Finally Been Hacked, And The Flaw Could Affect Millions Of Phones. Forbes. 21 de julio de 2013 http://www.forbes.com/sites/parmyolson/2013/07/21/sim-cards-have-finally-been-hacked-and-the-flaw-could-affect-millions-of-phones/

[71] BARLOW, John Perry. Declaración de Independencia del Ciberespacio. http://www.uhu.es/ramon.correa/nn_tt_edusocial/documentos/docs/declaracion_independencia.pdf

[72] BRUNVAND, Erik. The Heroic Hacker: Legends of the Computer Age, Department of Computer Science University of Utah. 15 de octubre de 1996. http://www.cs.utah.edu/~elb/folklore/afs-paper/node3.html

[73] DE SALVADOR CARRASCO, Luis. Redes de anonimización en Internet: cómo funcionan y cuáles son sus límites Documento de opinión IEEE 16/2012 http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO16-2012_RedesAnonimizacionInternet_LdeSalvador.pdf

[74] GARCÍA GUERRA, Miguel Ángel. Educación y nuevas tecnologías Nuevo verbo: 'trolear'. 19 de febrero de 2012 http://www.magarciaguerra.com/2012/02/nuevo-verbo-trolear/

dentro de unos límites; y de que hay que asumir las responsabilidades cuando esos límites se traspasan. Además, no podemos olvidar que la red tiene memoria, como nos demuestran a diario los buscadores; y la opinión que hoy se publica, mañana puede traer consecuencias indeseadas.

Ejemplos como la Primavera Árabe nos enseñan que los fenómenos de ciberactivismo tienen una mayor fuerza desestabilizadora y son más susceptibles de manipulación, en algunos casos con consecuencias catastróficas, en aquellos lugares donde la estructura democrática se ha debilitado o no existe. El ciberactivismo no hay que combatirlo por si mismo, es un síntoma. Los fenómenos como Wikileaks no son nuevos, los casos "Pentagon Papers" o el Watergate tuvieron características similares. Estos últimos surgieron en el marco de un gobierno que se debilitó cuando actuó al margen de la ley. La mejor defensa contra los abusos del ciberactivismo es fortalecer el Estado de Derecho, en el que sus instituciones, medios de comunicación y estructura social sean realmente libres, plurales, sujetos a la ley, independientes entre sí, y en el que cada ciudadano no se sienta empujado a ejercer de policía, periodista y fiscal.

LOS FENÓMENOS RELÁMPAGO Y LA REALIMENTACIÓN DE LA DESINFORMACIÓN

¿Es posible que una entrada en un blog francés que habla de ciencias ocultas[75] y que pronostica un maremoto provoque el terror y el éxodo en la ciudad de Casablanca? Así parece que sucedió en 2006, al menos con la suficiente intensidad para que fuese informado por el cónsul norteamericano[76] y para generar declaraciones del responsable de los servicios meteorológicos marroquíes. Otro caso de propagación de bulos con graves consecuencias tuvo lugar en el año 2011, en la localidad mexicana de Veracruz. Mediante Twitter se propagaron mensajes falsos que informaban sobre avisos de bomba en varios colegios de la ciudad, lo que generó una ola de pánico que se propagó en la red social con un efecto dominó. El resultado fueron decenas de accidentes automovilísticos cuando los padres, desesperados, acudieron a salvar a sus hijos de las escuelas, colapsándose además las líneas telefónicas de emergencia[77].

[75] JULIEN, Éric Julien, To understand the tsunami of may 25, 2006 Oeuvres, Visions, News, Intel. 21 de noviembre de 2012 http://ericjulienovni.blogspot.com.es/2012/11/to-understand-tsunami-of-may-25-2006.html#more

[76] WIKILEAKS. Tsunami destroys Casablanca - next thursday http://www.wikileaks.org/plusd/cables/06CASABLANCA571_a.html

[77] Sin firma. Los 'twitterroristas' de México se enfrentan a 30 años de cárcel. El Mundo, 5 de septiembre de 2011. http://www.elmundo.es/america/2011/09/05/mexico/1315239774.html

Como en el caso de Wells en la "Guerra de los Mundos", el impacto que tuvieron esos fenómenos se debió en gran medida a la falta de madurez, tanto del canal de comunicaciones como de los ciudadanos en relación a su capacidad de análisis crítico de los mensajes que reciben. Los medios y las estrategias de comunicación tienen un ciclo de vida. Cuando se despliegan por primera vez, tienen un corto periodo experimental en el que crean nuevas formas de lenguaje, que, al evolucionar, generan gran impacto social, llegando incluso a anclarse en la memoria colectiva. En relación a los ejemplos mostrados más arriba, sería difícil repetir actualmente el éxito de la formula blog, realizado en 2006, mientras que el canal Twitter aún conserva su capacidad de impacto.

La repetición de la misma fórmula, la saturación de los sujetos receptores[78], la diversificación de fuentes, la segmentación del público, la fiabilidad o la credibilidad otorgada a los autores,, hacen que nuevos mensajes utilizando viejas fórmulas no alcancen el mismo éxito de la original[79], aunque sí puedan conservar un nicho de incondicionales. En el caso de las redes sociales, en una reciente mesa redonda se declaraba que los generadores de opinión en las mismas eran en un 80% periodistas que ya tenían columnas en otros medios[80], lo que nos da una idea de la madurez que ha alcanzado dicho canal.

Esto no significa que Internet, o en un sentido más amplio las tecnologías de la información, sean ya un medio maduro y estable; todo lo contrario. La experiencia de los últimos veinte años nos enseña que, continuamente, se han ido creando nuevas estrategias de comunicación en Internet. Desde que surgieron las BBS y más tarde las news, correos electrónicos, páginas web, blogs, redes sociales, tweets.... siempre se ha encontrado alguien con imaginación para reinventar un nuevo canal de comunicación.

En abril de 2013, el índice industrial Dow Jones cayó 143 puntos después de que hackers enviaran un mensaje en Twitter utilizando el usuario de la agencia de noticias Associated Press. En dicho tweet, se decía que la Casa Blanca había sido alcanzada por dos explosiones y que Barack Obama había resultado herido[81]. Aunque el tweet fue inmediatamente corregido por la agencia, fue reenviado casi dos mil veces, con un efecto avalancha[82].Este es un caso

[78] Por ejemplo, La estafa que se producía mediante el mensaje SMS "Alguien quiere conocerte" tuvo una vida de éxito que se prolongó entre 2007 y 2009. La sobreexplotación de la misma fórmula y la saturación de los receptores la han dejado en un fenómeno residual.
[79] Existen fórmulas que se reinventan, el conocido "timo del nigeriano" se denomina en el siglo XVI la "carta del prisionero español".
[80] MOYANO, Ícaro. Mesa redonda: “Activismo en la Red: nuevas reglas del juego en la movilización social”, Mas Consulting Group, Febrero de 2013
[81] MOORE, Heidi. AP Twitter hack causes panic on Wall Street and sends Dow plunging. Market recovers after hackers tweeted from the official AP feed that two explosions had hit the White House 23 The Guardian, 23 de abril de 2013 http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall
[82] Sin firma. AP Twitter Hack Claims Obama Injured In White House Explosion. The Huffington Post Canada 23 de abril de 2013 http://www.huffingtonpost.ca/2013/04/23/ap-twitter-hack-claims-ob_n_3140451.html

real de cómo funcionan los fenómenos relámpago en la red, y de cómo la rápida realimentación de estados emocionales generan presión sobre órganos de decisión que se ven forzados a actuar en un plazo muy corto.

Los ejemplos de este apartado muestran cómo en la era de la información, de forma paradójica, se toman decisiones utilizando muy poca información, sin realizar un análisis crítico o sin contrastarla. Más que una era de información, es una era de datos. Como tal, existe un peligro real de que se adquiera el control de los medios para algo más serio que una broma, como crear un ambiente caldeado –aunque sea por un corto periodo- que destierre el análisis sosegado[83]. Algo que, tradicionalmente, estaba asociada a estados autoritarios o a la existencia de poderosos grupos económicos que controlaban los medios.

Actualmente, están también volcados en Internet, y sometidos por tanto a una mayor presión competitiva y, de esta forma, los tiempos de edición de las noticias publicadas tienden a cero[84]. A esto se une el hecho de que hay medios alternativos que no ejercen ningún tipo de autocrítica sobre la calidad de la información distribuida, ni un juicio sereno que contraste su veracidad o que evalúe las consecuencias de distribuirla en un momento dado. El mecanismo actual de generación de contenidos ha sufrido un proceso de desintermediación y ya no es necesaria la edición en una redacción informativa. Incluso los receptores de la información se convierten en editores, propagándola, no necesariamente en su literalidad, sino adaptándola en función de sus esquemas o intereses, en mensajes, blogs, redes sociales, etc. El grado de conectividad de los ciudadanos es elevadísimo, tanto en sus roles profesionales como privados, influyéndose entre ellos. La entrada masiva de elementos de información reclama, a su vez, la respuesta inmediata, la reacción emocional. No hay tiempo para pensar. Esto permite que los estados de opinión se propaguen de forma explosiva y a gran velocidad[85].

Este esquema permite que la difusión de noticias no sea unidireccional, de los medios a los ciudadanos, sino que éstos se realimentan en tiempo real del supuesto impacto que tienen sobre los sujetos. Entre ellos se encuentran quienes ocupan puestos de responsabilidades, en la estructura del Estado o en la económica. Todos ellos se alimentan

[83] DE SALVADOR, Luis,. *Ingeniería social y operaciones psicológicas en Internet*. Documento de opinión IEEE 74/2011 http://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO74-2011.IngenieriaSocial_LuisdeSalvador.pdf

[84] Sin firma. EL PAÍS retira una falsa foto de Hugo Chávez. La foto que EL PAÍS nunca debió publicar. El País 24 enero 2013 http://internacional.elpais.com/internacional/2013/01/24/actualidad/1359002703_817602.html

[85] MELLADO, Ana. Una demanda contra 10.000 tuiteros, ABC, 3 de abril de 2013 http://hemeroteca.abc.es/nav/Navigate.exe/hemeroteca/madrid/abc/2013/03/03/049.html

del estado de opinión del público, y están más presionados para adoptar respuestas sobre la marcha, influenciados en su toma de decisiones o en gestos públicos[86].

El sistema aquí reflejado es un ciclo realimentado que en un momento dado puede descontrolarse si se amplifica con su propia salida; si la propagación de estados emocionales entra en resonancia. Por supuesto, la propagación incendiaria de noticias o bulos no es nada nuevo. La gran diferencia estriba en la extensión y velocidad explosiva de las comunicaciones que han cambiado los ritmos y tiempos de reacción, y el descontrol sobre los mecanismos de generación de información.

La realidad es que no hay una mínima protección ni sobre los contenidos que se vuelcan en estos medios ni sobre las consecuencias que podrían tener. Aunque es muy difícil introducir mecanismos de regulación que no tengan el carácter de censura previa, es necesario tomar medidas para evitar el uso inconsciente de dichos medios. Es más, es necesario prevenir que nadie pueda tomar su control unilateralmente y, de la misma forma que se ha de garantizar la libertad en las calles frente acciones de fuerza, también se han de evitar las maniobras de manipulación en la red. Ya se han planteado medidas como la monitorización de los estados de opinión, el seguimiento de "trending topics", la prevención de la utilización de técnicas de posicionamiento en buscadores, la utilización de filtros "paso bajo" para evitar los efectos avalancha o la detección del uso de técnicas de psicología de masas[87]. Es importante esta supervisión, el control transparente de la misma supervisión (vigilar al vigilante), el planteamiento de hipotéticas situaciones de crisis y el estudio sistemático de los posibles nuevos escenarios que crean los nuevos hábitos de comunicación y las nuevas herramientas.

ALDEA GLOBAL, REGULACIÓN LOCAL

Uno de los aspectos por el que las redes de comunicación resultan de capital importancia es el desplazamiento de actividades económicas tradicionales al terreno virtual. En Internet han surgido nuevos modelos de negocio de alcance global y de gigantescas dimensiones pero, a la vez, el mismo comercio local se ha incorporado a la utilización de los nuevos canales de publicidad, distribución y venta. Las relaciones establecidas de esta forma entre clientes (finales o no) y proveedores necesitan ser reguladas, y están siendo reguladas, tanto

[86] Un ejemplo ficticio ilustrativo de la realimentación de los estados de opinión aparece en el siguiente video publicitario de The Guardian: El anuncio de Los Tres Cerditos. http://incirtv.wordpress.com/2012/03/29/el-anuncio-de-los-tres-cerditos-de-the-guardian/

[87] DE SALVADOR CARRASCO, Luis. Ingeniería social y operaciones psicológicas en Internet, Documento de opinión IEEE 74/2011, 2011 http://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO74-2011.IngenieriaSocial_LuisdeSalvador.pdf

para proporcionar una seguridad jurídica a sus actores como para someterse a las autoridades de control de todo tipo: sanitarias, comerciales o fiscales.

Dentro del Espacio Económico Europeo ha ido creciendo el aparato normativo y sancionador sobre las actividades económicas que se realizan a través de la red. Esta regulación es del orden administrativo, civil y penal con el objeto de proteger los derechos de los ciudadanos en relación a su privacidad, el comercio electrónico, la publicidad, la protección de menores, la confidencialidad de las comunicaciones, las estafas y toda clase de delitos relacionados con estas actividades. Todo ello impone unas obligaciones onerosas a aquellas empresas que están radicadas en nuestro país, ya que el respeto de los derechos tiene, entre otros, influencia en los costes de desarrollo o la pérdida de cuotas de mercado[88].

La naturaleza global de Internet ha creado un marco de desigualdad entre las empresas oficialmente radicadas en nuestro país y aquellas que ofrecen sus servicios desde paraísos fiscales, o en países que no ofrecen las necesarias garantías. Estas escapan a la aplicación directa del aparato normativo de nuestro país y pueden ejercer sus actividades poniendo a nuestros ciudadanos en un plano de indefensión legal[89], escapando a la tributación española[90] y aplicando a sus trabajadores regímenes sin ningún tipo de protección. Gran parte de los contratos o condiciones de servicio de estas empresas obligan a los usuarios de nuestro país a someterse a normativas extranjeras y a renunciar a los más elementales derechos.

La aplicación de distintas regulaciones según estén localizados los servicios proporciona a los usuarios la ilusión de que existe una especie de "libertad en Internet". El concepto resulta atractivo en un primer momento y existe una tendencia a oponerse a cualquier forma de control aduciendo el peligro de caer en la censura. Pero "la red sin fronteras" ha derivado hacia una Internet con fronteras, pero sólo para la protección efectiva de los derechos, en particular de algunos derechos fundamentales de los ciudadanos. Hay que preguntarse hasta dónde llega esa supuesta libertad si mis comunicaciones pueden ser leídas por un gobierno extranjero, los servicios que utilizo suspendidos sin que se respeten obligaciones contractuales, mis dispositivos catalogados, rastreados y relacionados para intereses

[88] MORENO, Irina. Óscar Casado, director legal y de privacidad de Tuenti: “Nuestra regulación nos deja en desventaja competitiva frente a empresas como Facebook”. Diariojurídico.com. 20 de febrero de 2013 http://www.diariojuridico.com/entrevista-destacada-2/oscar-casado-director-legal-y-de-privacidad-de-tuenti-nuestra-regulacion-nos-deja-en-desventaja-competitiva-frente-a-empresas-como-facebook.html

[89] EuropaSur.es. Gibraltar potenciará con un cable submarino sus telecomunicaciones. Gibtelecom forma parte del consorcio que desarrollará el sistema de fibra óptica entre el Reino Unido e India · Carracao cree que el Gobierno español no pondrá trabas al proyecto pese a la disputa por las aguas. 30.08.2009 http://www.europasur.es/article/gibraltar/502805/gibraltar/potenciara/con/cable/submarino/sus/telecomunicaciones.html

[90] JIMÉNEZ, Miguel. Los siete gigantes de Internet pagan en España sólo un millón en impuestos. El País, 18 de enero de 2014 http://economia.elpais.com/economia/2014/01/18/actualidad/1390071860_568641.html

comerciales, los menores utilizados y todo ello sin poder reclamar una protección legal efectiva.

Precisamente, gobiernos como China y Rusia, en los que existen paraísos para ejercer actividades ilegales en la red, son los que desean reemplazar el marco regulatorio global en Internet por un sistema estructurado, dirigido por los gobiernos y bajo la regulación de la ONU[91], más específicamente del ITU, organización que está intentando tener un rol más prominente en la regulación de la red. Este no es el tipo de control que garantiza los derechos y libertades de ciudadanos y personas jurídicas, sometido al imperio de la ley, sino otro muy diferente, el que limita la privacidad, restringe la libertad de expresión y permite la vigilancia indiscriminada de los ciudadanos, los suyos y los nuestros, mientras posibilita condiciones de competencia desleal.

Las condiciones expuestas en los párrafos anteriores son inaceptables, teniendo en cuenta que afectan a nuestra infraestructura comercial y a nuestra privacidad. Por lo tanto, aquellos servicios que se prestan a ciudadanos españoles en régimen de monopolio de facto o que tienen altos grados de implantación en el conjunto de personas físicas o jurídicas de nuestro país tienen que estar supeditados a las autoridades regulatorias españolas. Más concretamente, cuando el volumen de tráfico o negocio en nuestro territorio tenga la suficiente entidad, se ha de obligar a tener establecimientos bajo nuestra directa competencia y protección con un doble propósito: el sometimiento a las leyes españolas y la existencia de instalaciones con las que prestar de forma local dichos servicios, que incluya sistemas y personal. Si no se cumplen dichos requisitos, es necesario restringir el tráfico desde y hacia países que no cumplen con unas mínimas garantías.

DE LA COMPLEJIDAD AL CAOS

En febrero de 2008 el gobierno pakistaní decidió que un video que se encontraba disponible en Youtube no era adecuado para la sensibilidad islámica de sus ciudadanos[92]. Ordenó a los proveedores locales de Internet el cierre del acceso al portal de videos para los usuarios de su propio país. El resultado de esta acción resultó inesperado, ya que el bloqueo local produjo una reacción en cadena que paralizó Youtube a escala global por varias horas, generando una publicidad indeseada.

[91] Internet's future on the agenda at Dubai meeting, IISS Strategic Comments, Volume 28, comment 44 de diciembre de 2012
[92] RIBEIRO, John. Pakistan causes worldwide Youtube blackout. MacWord. 25 de febrero de 2008. http://www.macworld.co.uk/news/apple/pakistan-causes-worldwide-youtube-blackout-20536/

Este es un ejemplo del grado de complejidad que han alcanzado las dependencias entre los sistemas en Internet. No sólo afecta a los servidores sino también a los dispositivos de los usuarios: gran parte de las aplicaciones que se emplean diariamente precisan estar conectadas permanentemente simplemente para que se inicien, buscando actualizaciones, parches de seguridad, una licencia, los datos del día a día, etc. Aparte de otras consideraciones, esto tiene un costo elevado en ancho de banda, un riesgo inherente de que se produzcan intrusiones, fallos de actualización o seguimiento de la actividad de los usuarios. La gestión de la complejidad en este entorno se convierte en un problema intratable. Según crecen las aplicaciones, redes y terminales conectados, el conjunto de relaciones y enlaces que se establecen se incrementa de forma no lineal sino exponencial.

Este sistema es tan complejo que se ha convertido en un sistema frágil e impredecible en el que se relacionan múltiples elementos: desde factores eléctricos a factores psicológicos, pasando por dependencias electrónicas y semánticas. Hay que tener en cuenta que las comunicaciones ya tienen algo más que un plano físico, sobre este se han construido numerosos planos lógicos (medios de comunicación, redes sociales, comercio electrónico, etc.) que derivan en una interdependencia que podríamos llamar multidimensional.

Para limitar dicha complejidad es necesario compartimentar servicios, independizando distintas áreas, garantizando zonas autónomas de funcionamiento y relocalizando los servidores cerca de los usuarios. Es necesario evitar que se solapen distintos niveles de protocolos y aplicaciones, y, por supuesto, que sus límites se correspondan con los límites nacionales o, al menos, regulatorios.

LA CIBERSEGURIDAD SOSTENIBLE

El gran dinamismo de la industria TIC ha permitido disfrutar de ventajas que se hacían impensables hace unos años. De forma simultánea, hemos asistido a las consecuencias de un crecimiento desordenado que ha generado varias crisis en lo económico y lo social. La evolución ha sido tan profunda que las TIC no son un añadido a nuestra sociedad, nuestra economía o nuestras infraestructuras, son parte integral de las mismas hasta tal extremo que, en algunos casos, constituyen la esencia de muchos sectores.

En este artículo se ha repasado un conjunto de factores estructurales (industriales, comerciales, técnicos y sociales) que influyen sobre nuestros sistemas de información y condicionan la efectividad de las políticas de ciberseguridad. Conseguir un marco real de seguridad exige un cambio cultural profundo a todos los niveles, un cambio de mentalidad en relación a cómo se entienden actualmente los sistemas de información y un

conocimiento profundo de las implicaciones de los cambios tecnológicos por parte de órganos decisorios en las empresas y en el Estado.

El gobierno de un elemento tan fundamental para el futuro de nuestra sociedad no se puede delegar en otros estados o empresas multinacionales, en intereses económicos a corto plazo, en opiniones de gurús mediáticos[93] o, lo que es peor, adoptar una postura simplemente reactiva frente a los vaivenes de las tendencias tecnológicas. Intentar implementar seguridad sobre estos supuestos es ir en contra del principio del núcleo de seguridad, es construir una casa sin cimientos.

La ciberseguridad pasa por disponer de una estructura TIC robusta, independiente y sostenible. Las vinculaciones exteriores son inevitables, pero eso no impide que se adopten estrategias de diversificación, intentando evitar los monopolios de facto, alentando un tejido industrial propio, controlando realmente la infraestructura estratégica, simplificando las interdependencias, utilizando una política de globalización racional y exigiendo la localización en nuestro país de determinados elementos clave. La política de información ha de estar guiada por la defensa de nuestros intereses como estado soberano, manteniendo un control predecible de nuestros recursos estratégicos a corto y a largo plazo, en el que se garanticen los derechos de los ciudadanos y su voluntad democráticamente expresada.

*Luis de Salvador Carrasco**
Doctor en Informática

[93] Como Vivek Kundra, autor de lo que se ha llamado el "Cloud First policy", dibujada en la Federal Cloud Computing Strategy, que centra sus esfuerzos en la migración global de los servicios estatales de cualquier país a la Nube, y asesor de la comisaria Neelie Kroes, vicepresidenta de la Comisión Europea responsable de la Agenda Digital Europea.

BIBLIOGRAFÍA

BALLESTEROS MARTÍN, Miguel Ángel. *Estudio prospectivo sobre la implementación del concepto "pooling and sharing" en el horizonte de 2020*. IEEE y TECNALIA. 2013

BAKER, Stewart. Et al. *En el punto de mira: las infraestructuras críticas en la era de la ciberguerra* McAffee. 2010

CANDAU ROMERO, Javier, *Líneas de acción de la Estrategia Nacional de Ciberseguridad*, Cuadernos de estrategia 149, IEEE 2010

CARO BEJARANO, Mª José, *Más sobre la Amenaza Cibernética* Documento de opinión IEEE 45/2013

CCN-CERT, *Informe de Amenazas Ciberamenazas 2012 y Tendencias 2013* CCN-CERT IA-09/13 2013

COMER, Douglas E., *Internetworking with TCP/IP. Vol I-II-III*, Prentice-Hall 2013

COMISIÓN EUROPEA, Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, *Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro* Bruselas, 2013

COMISIÓN EUROPEA, Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation,* 2013

COLE Ray, et al. *Social engineering: the human element in information warfare* CS4235A Information Warfare Group

CORTADA DE KOHAN Nuria, Los sesgos cognitivos en la toma de decisiones, International Journal of Psychological research 2008, ISSN: 2011-7922

DE SALVADOR, Luis,. *Ingeniería social y operaciones psicológicas en Internet*. Documento de opinión IEEE 74/2011

ENISA, *Cybersecurity cooperation, Defending the digital front-line, European Union Agency for Network and Information Security Science and Technology*, octubre 2013

GOLLMANN, Dieter. *Computer Security*. John Wiley & Sons, 2010

HARTWIG, Robert P., *Cyber Risks: The Growing Threat*, Insurance Information Institute, 2013

LEJARZA ILLARO, Eguskiñe, *Estados Unidos - China: Equilibrio de poder en la nueva ciberguerra fría* IEEE Documento de Opinión 60/2013

PRESIDENCIA DE GOBIERNO. *Estrategia de Ciberseguridad Nacional*. 2013

PRESIDENCIA DE GOBIERNO. *Estrategia Española de Seguridad*. 2011

PUYOL MONTERO, Javier. *Algunas consideraciones sobre Cloud Computing*. Boletín Oficial del Estado. 2013

SINGH, Simon, *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography,* Doubleday Books, 1999

TANENBAUM, Andrew S., *Computer Networks*, Prentice-Hall 2011

TIKK, Eneken, et al. *International Cyber Incidents, Legal Considerations*. CCDCOE Estonia, 2010 http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

WAINER, Tim. *Legacy of ashes*. First Anchor Books, 2008

i

---

*__NOTA:__ Las ideas contenidas en los ***Documentos Marco*** son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.