ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

86/2016 19 de agosto de 2016

*Joaquín Ruiz Díaz**

Ciberamenazas: ¿el terrorismo del futuro?

Ciberamenazas: ¿el terrorismo del futuro?

Resumen:

La información es actualmente un activo muy valioso, cuyo uso puede ser objetivamente legal y legítimo, pero que también puede ser utilizada con fines criminales, lo que ha dado origen a una delincuencia cibernética que puede tener un coste en términos económicos y de seguridad muy importante.
A través de Internet, no sólo circula información privada de personas o empresas de todos los sectores de la economía o la industria. Por esa inmensa tela de araña global, también circula información perteneciente a los Estados y las Administraciones Públicas, que en muchas ocasiones se trata, además, de información sensible o de control de infraestructuras críticas y sistemas de seguridad y defensa.
Para los terroristas, el conocimiento y la captura o control de esta información y los recursos que pueden ser manejados a través de ella, constituyen una amenaza para la sociedad que es necesario prevenir y combatir, ya que los daños ocasionados por una utilización con fines terroristas de la misma, puede suponer una escalada importante de la amenaza, que se materialice en atentados de consecuencias imprevisibles, pero mucho más graves que las que hemos sufrido hasta ahora.
Estamos asistiendo a una importante transformación, no sólo de nuestras formas de relacionarnos a nivel individual, sino también a las maneras de dirimir conflictos entre estados. En este sentido, las nuevas formas de ciberinteligencia y ciberguerra son dos aspectos a considerar muy atentamente de cara al futuro próximo.

Abstract:

Today information is a valuable asset, the use of which can, objectively, be legal and legitimate, but it can also be used for criminal purposes, which has given rise to cybercrime, which may have a very significant cost in economic and security terms.
It is not only the private information of individuals or companies from all sectors of the economy or industry that circulates over the internet. Information belonging to states and public authorities, which, moreover, is often sensitive information or critical infrastructure and safety and defence systems control, also circulates over this immense global web.
For terrorists, knowledge and capture or control of this information and the resources that can be managed through it, constitute a threat to society that must be prevented and combatted, since the damage caused through its use by terrorists could mean a significant escalation of the

threat that it may lead to attacks with unpredictable consequences, much more serious than any we have suffered so far.
We are witnessing a major transformation, not only in our ways of relating to one another individually, but also in the ways of settling disputes between states. In this sense, the new forms of cyber intelligence and cyberwarfare are two aspects to be considered very carefully in the near future.

Palabras clave:

Ciberseguridad, ciberterrorismo, ciberamenaza, Internet, ciberespacio, ciberinteligencia.

Keywords:

Cybersecurity, cyberterrorism, cyber threat, World Wide Web, cyberspace, cyber intelligence

Las ciberamenazas del siglo XXI

Podríamos definir las ciberamenazas, como aquellas actividades realizadas en el ciberespacio, que tienen por objeto la utilización de la información que circula por el mismo, para la comisión de distintos delitos mediante su utilización, manipulación, control o sustracción. Puesto que el ciberespacio es el escenario dónde se desarrollan las amenazas cibernéticas conviene conceptualizar, previamente, el mismo.

Para el Departamento de Defensa de los EE.UU. el ciberespacio sería "Un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores"[1].

La Comisión Europea lo define como "el espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo"[2] y por último la UIT (Unión Internacional de las Telecomunicaciones) define el ciberespacio como el lugar creado a través de la interconexión de sistemas de ordenador mediante Internet.

El uso del ciberespacio en el entorno terrorista, ha experimentado un importante crecimiento que se mantiene constante, sobre un medio, como Internet, que se ha demostrado vulnerable. En consecuencia, la red de redes se ha convertido tanto en un instrumento, como en un medio para los terroristas. Un instrumento para la captación y la radicalización y un medio de propaganda de sus actos terroristas.

Si además de un medio y un instrumento, se convierte también en un objetivo de sus acciones, lo cual aunque de momento se trata de una posibilidad, puede llegar a darse en el caso de que los entornos de los caminos de los *hackers* y de los terroristas confluyan, tendríamos que dejar de hablar de riesgos para plantearnos el problema como una amenaza real[3].

Uno de los factores que agravan el problema, es la visibilidad parcial de Internet, esto es, que exista una "Internet profunda" cuyo tamaño estimado es 500 veces mayor que

---

[1] Caro Bejarano, María José; "Alcance y ámbito de la seguridad nacional en el ciberespacio"; Instituto Español de Estudios Estratégicos; Cuadernos de Estrategia nº 149; 2011 Pág. 54; Citando a Joint Publication 1-02. Department of Defense. Dictionary of Military and Associated terms. (2009) [on line], http://www.dtic.mil.

[2] *Ibid*; Pág. 54 citando a European Commission. Glossary and Acronyms (Archived). In Information Society Thematic Portal, http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c

[3] Fernández García, Luis; "Nuevas Ciberamenazas del siglo XXI"; Ciberterrorismo, hacktivismo, cibercrimen, ciberespionaje y ciberguerra; Master en Análisis y prevención del terrorismo; URJC; 2016

la Internet superficial. Esto supone que los buscadores tradicionales solo son capaces de detectar un 1% del contenido existente en internet. Las VPN, o redes privadas virtuales, como TOR[4] o I2P, que permiten la navegación anónima, tanto por el internet conocido como por el profundo resultan un peligro para la seguridad de muy alto nivel[5].

Este tipo de herramientas refuerza el anonimato de la navegación, impidiendo localizar al internauta que está accediendo, ya que la dirección IP[6] del mismo, queda encubierta por sucesivos cambios de servidores por donde pasan los paquetes de datos, lo cual hace muy difícil su monitorización y localización.

La vasta expansión del ciberespacio —no solo en términos de usuarios, sino de contenido y aplicaciones— ha conllevado un nuevo conjunto de amenazas y desafíos jamás previstos por los diseñadores de la red. En los inicios de esta revolución tecnológica, el acceso se materializaba solo a través de unas pocas computadoras centrales conectadas; literalmente, no había nada que robar o atacar, y no había ninguna infraestructura conectada a la red. La ciberseguridad, por tanto, no era un tema de discusión[7].

Con el tránsito a Internet a escala mundial y la evolución del comercio electrónico, al igual que la amplitud y variedad de sus contenidos, el ciberespacio se convirtió en un escenario, en la medida en que los servicios militares y de inteligencia se convirtieron en principales usuarios de la red. Este nuevo mundo presenta desafíos que hay que atender[8].

Entre las posibles ciberamenazas se encuentran el ciberterrorismo, el “hacktivismo”, el ciberdelito, el ciberespionaje y la ciberguerra.

---

[4] Acrónimo de *The Onion Router*. Mediante la instalación de este programa, se accede a una red virtual de colaboradores que prestan sus equipos para que los paquetes de datos de otros usuarios sean redireccionados y de esta forma parezcan ser enviados desde otra dirección IP distinta de la del usuario de origen.

[5] Sánchez Medero, Gema; “El ciberterrorismo. De la web 2.0 al internet profundo.”; Revista Ábaco 2ª Época Volumen 3 Número 85 / 2015; ISSN: 0213-6252; Págs. 100-108

[6] Acrónimo de *Internet Protocol*. Se trata de un identificador único dentro del rango de direcciones de Internet, asignado por el proveedor de servicios contratado por el usuario y que identifica al mismo unívocamente. Puede tratarse de una dirección dinámica, lo más común, que se asigna aleatoriamente al usuario cuando este se conecta, o estática, esto es, una dirección fija permanente.

[7] Wagner, Abraham; “La seguridad nacional estadounidense y las tecnologías de la información”; Revista Temas nº 81-82 Págs. 25-32; 2015; Traducción David González; Pág. 26

[8] *Ibíd*.; Pág. 27

El ciberterrorismo constituye una de las amenazas más preocupantes, dado que sus consecuencias pueden suponer una escalada considerable de la gravedad de los atentados terroristas. Conviene pues definir el concepto de ciberterrorismo y los riesgos que conlleva, puesto que dentro del mismo existen diversos enfoques, ya que no sería lo mismo definirlo desde un punto de vista legal, que desde el punto de vista de las fuerzas de seguridad o desde el de los representantes de los gobiernos y Organismos Internacionales.

De acuerdo con la legislación, serían delitos de ciberterrorismo aquellos en los que el delincuente principalmente busca crear terror y atemorizar a amplios sectores de la población, mediante el uso de las nuevas tecnologías, cuando se hagan con fin terrorista.

Desde el punto de vista de los organismos de seguridad, "el ciberterrorismo se puede definir como el realizado por medios cibernéticos. Aunque esta definición no sólo se extiende al objetivo último de estos grupos sino al empleo de Internet para conseguir los mismos"[9].

De acuerdo con esta definición podemos concluir que, el ciberterrorismo podría no sólo utilizar el ciberespacio para conseguir sus objetivos, sino que este podría ser en un momento determinado el "objetivo" de los terroristas.

Para Javier Candau, "las actividades del terrorismo nacional e internacional en el ciberespacio se ciñen principalmente a lo especificado en el apartado anterior y su capacidad de realizar ciberataques a sistemas conectados a Internet es considerada limitada"[10]. Aunque este mismo autor, consideraba poco probable que los terroristas realizaran ataques a gran escala en el ciberespacio, no debemos perder de vista la rápida evolución de todo lo que tiene relación con las tecnologías de la información y la comunicación, y su uso cada vez más intensivo, tanto por parte de empresas privadas como también por las administraciones de los Estados, incluidas sus infraestructuras y sus dispositivos defensivos.

[9] Candau Romero, Javier; "Estrategias nacionales de seguridad. Ciberterrorismo"; Instituto Español de Estudios Estratégicos; Cuadernos de Estrategia nº 149; 2011; Págs. 259-322.

[10] *Ibíd.*; Pág. 265

En esta línea se puede observar cómo, especialmente a partir de los atentados del 11-S, tomó fuerza el concepto de ciberterrorismo como amenaza global. Actualmente éste se ha visto desplazado a un nuevo concepto globalizador, definido como ciberamenazas, para combatir las cuales es necesario articular protocolos de ciberseguridad[11].

El ciberterrorismo alcanzaría su auténtico significado, cuando no fuera únicamente un medio, sino el objetivo del ataque terrorista, orientándose hacia las acciones ofensivas contra los sistemas de información y comunicaciones, que sustentan el normal funcionamiento de las Infraestructuras Críticas y Estratégicas y cualquier otro servicio esencial para la ciudadanía[12].

No obstante, el último resumen ejecutivo del CERT del CCN, (Computer Emergency Response Team del Centro Criptológico Nacional) con datos de 2015 y tendencias para 2016, tampoco considera al ciberterrorismo por el momento una grave amenaza, a causa de las limitadas capacidades técnicas observadas en sus despliegues, aunque si apunta al crecimiento de la peligrosidad potencial de sus acciones atribuibles[13].

La llegada a este punto sería especialmente preocupante, por la importancia de las consecuencias que podrían suponer, las acciones dirigidas contra infraestructuras críticas, como aeropuertos, centrales nucleares, instalaciones de seguridad y defensa o de la Administración del Estado. Su importancia está justificada, en base a su inclusión en el capítulo tercero de la Estrategia de Seguridad Nacional. En ella, entre otros riesgos y amenazas, se encuentra la vulnerabilidad de las infraestructuras críticas y servicios esenciales. “Los riesgos y amenazas que se ciernen sobre las infraestructuras críticas españolas son múltiples. Su origen puede ser natural o inducido por errores humanos o fallos tecnológicos inesperados. Sin embargo, son los que se causan deliberadamente, bien por una agresión de carácter físico o por un ataque cibernético, los que revisten mayor peligrosidad, puesto que su móvil y objetivos consisten en ocasionar un daño grave a España y a sus ciudadanos”[14].

---

[11] Hernández García, Luis; “Ciberseguridad; respuesta global a las amenazas cibernéticas del siglo XXI”; Págs. 6-36 en Cuadernos de la Guardia Civil nº 49; Dirección General de la Guardia Civil; Ministerio del Interior; ISSN 2341-3263; Madrid; 2014, Pág. 10

[12] *Ibíd*.; Pág. 14

[13] CCN-CERT IA-0916_Ciberamenazas_2015_Tendencias_2016_Resumen_Ejecutivo; Pág. 9

[14] Estrategia de Seguridad Nacional; Capítulo 3 Apartado 12; Obtenido de

En la actualidad, los grupos terroristas, especialmente los de carácter radical, utilizan el ciberespacio fundamentalmente para labores de propaganda, adoctrinamiento y captación, pero de cara a una previsible evolución de su estrategia, un ataque dirigido a la toma de control de alguna de las infraestructuras críticas mencionadas, podría ocasionar daños de una gravedad extrema, cuya repercusión podría superar con creces la de atentados pasados, tanto en daños humanos como materiales, máxime teniendo en cuenta que hoy en día a través de internet y de las redes de datos privadas de empresas y gobiernos, circula información que es sensible para la seguridad nacional de la mayoría de los países occidentales.

El "hacktivismo" podría definirse como la fusión del *hacking* y el activismo. El *hacker* sería la persona que se dedica a explorar los detalles de los sistemas informáticos, estudiando como ampliar sus funcionalidades, mientras que el activista practica la acción directa militante para una meta social o política[15].

Se pueden distinguir dos categorías de "hacktivistas": la primera los que podríamos denominar profesionales, que buscan el fomento de la utilización del software libre, en contraposición al código por licencias de uso, y que estaría formado por profesionales de las TIC, con amplios conocimientos de programación. El segundo grupo, serían aquellos que buscan la utilización del espacio informático, como un medio propagandístico para promover la justicia social.

Aunque el término parezca nuevo, su origen se remonta a los comienzos de Internet, y a los grupos propulsores del acceso libre y universal a las computadoras, a la información y a la privacidad.

Los inicios del movimiento se remontarían al comienzo de la década de los 80 del pasado siglo y experimentarían un salto cualitativo en 2003 con la aparición en escena de Anonymus y las filtraciones de WikiLeaks, momento en que se observa también un cambio en la forma de llevar a cabo las acciones – centradas fundamentalmente en

http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf; consultado el 4-5-2016

[15] Mayorga Martin, José Luis; "Hacktivismo"; Págs. 37-54 en Cuadernos de la Guardia Civil nº 49; Dirección General de la Guardia Civil; Ministerio del Interior; ISSN 2341-3263; Madrid; 2014, Pág. 39

ataques DoS/DDoS[16] o modificaciones de páginas Web – pasando al acceso y difusión de datos confidenciales.

La aparición de la ciberdelincuencia

Dentro de la ciberdelincuencia, se engloban una serie de actuaciones, definidas por el Consejo de Europa en su Convenio sobre la ciberdelincuencia promulgado el 23 de noviembre de 2001 en Budapest y ratificado por España en el año 2010.

En el mismo se relacionan una serie de actividades realizadas en el ciberespacio, dirigidas a diversos objetivos, que por su naturaleza serían constitutivos de delito. Un breve resumen de los mismos, sería el siguiente:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, como:
  - ✓ Acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema y abuso de los dispositivos.
- Delitos informáticos, entre los cuales:
  - ✓ Falsificación informática o fraude informático.
- Delitos relacionados con el contenido:
  - ✓ Pornografía infantil (producción, puesta a disposición, difusión, adquisición o posesión de la misma por medio de un sistema informático)
- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines[17].

[16] Acrónimo de *Denial of Service / Distributed Denial of Service*. Se entiende como Denegación de Servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo, sobrecargándolo con un elevado número de peticiones simultaneas, hasta que éste no puede atenderlas, provocando su colapso y de esta forma no permitir que sus legítimos usuarios puedan utilizar los servicios por prestados por el.

Un método más sofisticado es el Ataque de Denegación de Servicio Distribuido (DDoS), mediante el cual las peticiones son enviadas, de forma coordinada entre varios equipos, que pueden estar siendo utilizados para este fin sin el conocimiento de sus legítimos dueños.

Esta última modalidad se consigue mediante el uso de programas malware que permitan la toma de control del equipo de forma remota, como puede ser en los casos de ciertos tipos de gusano o bien porque el atacante se ha encargado de entrar directamente en el equipo de la víctima. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html.

Definición de http://www.inteco.es/glossary/Formacion/Glosario/

Las consecuencias más significativas de este tipo de delitos son las económicas y las de reputación, aunque por supuesto no debemos restar importancia a los relacionados con el contenido, los cuales suponen un ataque a la dignidad y los derechos fundamentales de las personas, especialmente deleznable en los relacionados con pornografía infantil.

Los ataques son cada vez más sofisticados y afectan redes informáticas que en teoría disponen de niveles de seguridad extremos.

A modo de ejemplo podemos citar los ataques producidos contra la plataforma SWIFT[18], la red internacional de comunicaciones entre bancos, por la que circulan diariamente millones de transferencias en todas las divisas.

El último conocido de estos ataques se llevó a cabo contra el Banco Central de Bangladesh, del que se sustrajeron 81 millones de dólares de dicha entidad depositadas en la Reserva Federal de Nueva York, que se transfirieron a Filipinas. Las órdenes de transferencia fueron realizadas con códigos auténticos del sistema, pertenecientes a empleados del banco, y ascendían a 951 millones de dólares, cifra que provocó que la Reserva Federal intentara reconfirmar las mismas con el Banco Central de Bangladesh, lo que no fue posible pues el ataque estaba programado para el fin de semana en Bangladesh. Al no poder confirmar las órdenes, la Reserva Federal sólo tramitó 5 de ellas, por el importe finalmente robado.

Cuando desde el banco tuvieron constancia del robo e intentaron comunicarse con la Reserva Federal tampoco fue posible, pues entonces era fin de semana en Nueva York[19].

Esto demuestra la exquisita planificación del ataque, que además se ve reforzado por la forma de hacer desaparecer el dinero, que fue enviado como hemos expuesto a Filipinas e ingresado en una red de casinos de esa nacionalidad. En este país las normas y regulaciones referentes a las transacciones financieras son extremadamente

[17] BOE nº 216 de 17 de septiembre de 2010. https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf

[18] Acrónimo de *Society for Worldwide Interbank Financial Telecommunication* (Sociedad para las Comunicaciones Interbancarias y Financieras Mundiales)

[19] Información obtenida de http://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html

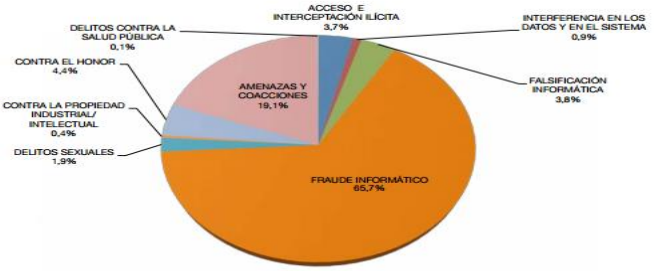
laxas y el secreto bancario colabora intensamente en los procesos de lavado y blanqueo de dinero.

La forma de proceder en este ataque es similar a otros dos ocurridos en Vietnam en diciembre pasado, que se frustro, y otro en enero del pasado año contra un banco de Ecuador del que lograron sustraer 9 millones de dólares. El denominador común, fue la plataforma SWIFT, desde donde se han reconocido varios ataques más, pero desde la misma insisten que su red, programas y servicios no se han visto comprometidos y lo que falló fueron los entornos internos de los bancos, entornos que, según el CEO de SWIFT Gottfried Leibbrandt, no pueden proteger desde su plataforma[20].

La siguiente imagen ofrece una muestra del crecimiento de este tipo de delitos en España en el periodo de 2011 a 2014.

CIBERCRIMINALIDAD Y PRINCIPALES TIPOLOGÍAS PENALES COMETIDAS CON LAS NUEVAS TECNOLOGÍAS

Grupos delictivos	2011	2012	2013	2014
Acceso e interceptación ilícita	1.492	1.701	1.805	1.851
Interferencia en los datos y en el sistema	228	298	359	440
Falsificación informática	1.860	1.625	1.608	1.874
Fraude informático	21.075	27.231	26.664	32.842
Delitos sexuales	755	715	768	974
Contra la propiedad industrial/intelectual	222	144	172	183
Contra el honor	1.941	1.891	1.963	2.212
Amenazas y coacciones	9.839	9.207	9.064	9.559
Delitos contra la salud pública	46	43	34	31
Total	**37.458**	**42.855**	**42.437**	**49.966**



Fuente: Anuario estadístico del Ministerio del Interior correspondiente a 2014. Fecha de edición: junio 2015. Consultado el 17 de mayo de 2016. http://www.interior.gob.es/documents/642317/1204854/Anuario-Estadistico-2014_v201510.pdf/0c18a800-f7f7-405c-9155-7391633618c8

[20] Información obtenida de https://www.swift.com/insights/press-releases/gottfried-leibbrandt-on-cyber-security-and-innovation y http://tecnologia.elpais.com/tecnologia/2016/05/25/actualidad/1464186438_489455.html consultadas el 26 de mayo de 2016

El análisis de la variación de los datos del cuadro anterior nos da una idea aproximada de la evolución del número de casos y de los porcentajes de casos resueltos y de los que se han saldado con detenidos.

	AÑO				DIFERENCIAS PORCENTUALES			
	2011	**2012**	**2013**	**2014**	**2011-12**	**2012-13**	**2013-14**	**2011-14**
CONOCIDOS	**37.458**	**42.855**	**42.437**	**49.966**	14,41	-0,98	17,74	33,39
ESCLARECIDOS	**S/D**	**15.066**	**16.414**	**17.948**	**S/D**	8,95	9,35	19,13
DETENCIONES	**S/D**	**5.057**	**5.101**	**5.573**	**S/D**	0,87	9,25	10,20
% Esclarecidos	S/D	35,16%	38,68%	35,92%				
% Detenciones	S/D	11,80%	12,02%	11,15%				

Fuente: elaboración propia partiendo de los datos de la imagen anterior.

Teniendo en cuenta que los datos se refieren únicamente a delitos conocidos, es decir denunciados, y que la mayoría de estos delitos no se denuncian, por ser de menor importancia o incluso por desconocimiento de que han sido sufridos, sobre las diferencias porcentuales absolutas, podemos concluir que, el número de delitos conocidos aumenta considerablemente (33,39%) en el periodo comparado (2011-2014), y en los interanuales, excepto entre 2012-13, que desciende levemente. El número absoluto de delitos esclarecidos y de detenciones, mantiene una tendencia alcista.

En lo que se refiere a las variaciones relativas de los casos esclarecidos y el número de detenciones, con respecto a los casos conocidos, vemos que el porcentaje de casos esclarecidos se eleva muy levemente entre el 2012 y el 2014 perdiendo la tendencia alcista observada entre 2012 y 2013, mientras que el porcentaje de detenciones desciende levemente en 2014, tras un leve repunte en 2013.

Podríamos concluir pues, que este tipo de delitos aumenta en términos absolutos de forma considerable, lo mismo que el número de casos esclarecidos, y también aumenta el número de detenciones, sin embargo, el porcentaje de casos esclarecidos en relación con los conocidos, disminuye tras el repunte de 2013 y el de detenciones continua desde 2012 con tendencia a la baja.

La conclusión final podría ser que la eficacia de las fuerzas de seguridad ha aumentado tanto en esclarecimientos como en detenciones, pero sin embargo el número de ciberdelitos crece muy rápidamente, lo que no permite mantener la ratio de esclarecimientos y detenciones, como sería lo ideal.

> "Siempre que quieras atacar a un ejército, asediar una ciudad o atacar a una persona, has de conocer previamente la identidad de los generales que la defienden, de sus aliados, sus visitantes, sus centinelas y de sus criados; así pues, haz que tus espías averigüen todo sobre ellos.
>
> Siempre que vayas a atacar y a combatir, debes conocer primero los talentos de los servidores del enemigo, y así puedes enfrentarte a ellos según sus capacidades."
>
> "La información previa no puede obtenerse de fantasmas ni espíritus, ni se puede tener por analogía, ni descubrir mediante cálculos. Debe obtenerse de personas; personas que conozcan la situación del adversario."
>
> Sun Tzu. El arte de la guerra

Ciberespionaje y ciberguerra

Ciberespionaje y ciberguerra son dos conceptos que están íntimamente interconectados. El objetivo del primero es la obtención de información, información de tipo principalmente estratégico, que hoy en día se encuentra almacenada electrónicamente, si bien bajo grandes medidas de seguridad, en los servidores de las instituciones de defensa y estratégicas, de la inmensa mayoría de los países del mundo.

La recomendación de Sun Tzu sigue vigente en la actualidad después de más de 2.000 años transcurridos desde que escribió su obra más conocida y utilizada no sólo en el ámbito militar, sino en los negocios y en la política. Lo que ha cambiado radicalmente es el medio de conocer al enemigo. Por supuesto se siguen utilizando personas en labores de espionaje, pero cada vez toman mayor protagonismo en estas labores de

obtención de información, las TIC. Estas serían actualmente los fantasmas los espíritus y los cálculos que Sun Tzu mencionaba en su obra.

Hoy en día, los ataques de ciberespionaje más sofisticados, son los desarrollados y ejecutados por las agencias de inteligencia militar. El objetivo es, como para Sun Tzu, el conocimiento del "enemigo", con el fin de adquirir no sólo ventajas militares, sino también de carácter político, comercial y económico[21].

De la realidad de esta ciberamenaza, tenemos ejemplos como Stuxnet, el gusano informático que acabo con el programa nuclear de Irán, mediante la infección y toma de control del software del PLC[22] de una quinta parte de sus centrifugadoras para enriquecer uranio, con el objeto de destruir las mismas. Aunque lógicamente no existe confirmación oficial, las principales empresas mundiales de seguridad informática apuntan a que el mismo fue supuestamente desarrollado conjuntamente por EE.UU. e Israel[23].

Otro ataque que pudo generar un conflicto diplomático internacional, fue el que supuso la captura en diciembre de 2014 de 5,6 millones de huellas digitales de la OPM[24] del gobierno de los EE.UU. El origen del mismo fue localizado en China, aunque no estaba claro el grupo u organización que lo desarrolló. En el ataque se vieron comprometidos datos de 22 millones de empleados públicos estadounidenses – en principio el número de huellas digitales reconocidos por la OPM como capturados era sólo de 1,1 millones – la agencia atacada minimizó el riesgo de la utilización de estos datos biométricos, pero todos los indicios apuntaban hacia la construcción por parte de China de una base de datos con información sobre funcionarios y contratistas estadounidenses. El reconocimiento de este ataque se hizo justo un día antes de la llegada del presidente Xi

---

[21] Candau Romero, Javier; "Estrategias nacionales de seguridad. Ciberterrorismo"; Instituto Español de Estudios Estratégicos; Cuadernos de Estrategia nº 149; 2011; Págs. 259-322; Pág. 269.

[22] Acrónimo de *Programmable Logic Controller*. Son los sustitutos desde los años 90 de los antiguos relés eléctricos.

[23] Según un reportaje de New York Times, el proyecto para retrasar lo más posible el programa nuclear iraní se inició en los últimos meses de mandato de George Bush. El presidente Obama lo mantuvo con la colaboración de Israel. EE.UU. e Israel eran los países más interesados en que Irán no consiguiera hacerse con el arma nuclear. Israel se había encargado de probar la efectividad del gusano Stuxnet en centrifugadoras de la compañía Siemens iguales a las utilizadas en Natanz por Irán. En 2008, esta compañía colaboró con un laboratorio estadounidense en la identificación de las vulnerabilidades de sus PLC.

Reportaje completo en: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

[24] Acrónimo de *Office of Personal Management* (Oficina de Gestión de Personal)

Jianping a Washington para una reunión con el presidente Obama, en la cual se trataría principalmente de la limitación del ciberespionaje[25].

Así ha nacido un nuevo concepto, el de «inteligencia económica» definido como: "el conjunto de acciones coordinadas de investigación, tratamiento y distribución de la información para tomar decisiones en el orden económico." Acciones que se dirigen tanto al ámbito de la economía nacional como en el dominio empresarial, pues la globalización de los mercados pone también en riesgo a las propias empresas[26].

El fenómeno del ciberespionaje, no sólo afecta a información de seguridad, también tiene una importantísima incidencia en el sector económico. Las grandes empresas multinacionales sufren igualmente el acoso de los espías electrónicos, en busca de información sobre nuevos proyectos de desarrollo, en un entorno altamente globalizado y competitivo.

A la obtención de esta información seguiría a continuación la utilización de la misma con fines estratégicos, mediante tácticas de ciberguerra. El ciberespacio – el quinto escenario de una guerra, además de los de tierra, mar, aire y espacio exterior – introduce un nuevo concepto alejado de las leyes de la guerra tradicionales y pone sobre la mesa una serie de preguntas acerca de cómo se desarrollarán las guerras futuras, pero las técnicas de ciberguerra, parecen claramente orientadas, a diferencia de las guerras tradicionales del siglo XX, donde estratégicamente el factor más importante era la conquista del territorio, a la dominación del mismo a distancia, mediante el control económico y tecnológico.

Las estrategias de defensa. El binomio ciberamenazas / ciberseguridad

Una vez demostrada la realidad de las ciberamenazas, será también oportuno repasar qué medidas se están tomando para neutralizarlas por parte de los distintos actores encargados de la prevención o represión de las mismas.

[25] Información obtenida de http://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html Consultada el 26 de mayo de 2016.

[26] OLIER, Eduardo; "Inteligencia estratégica y seguridad económica", en Cuadernos de Estrategia 162; La inteligencia económica en un mundo globalizado; Instituto Español de Estudios Estratégicos; IEEE; Ministerio de Defensa; 2013; Págs. 9-31; Pág. 11.

La ciberseguridad es el conjunto de medidas, de carácter técnico o no, que se encargan de proteger tanto la parte concerniente a las infraestructuras globales, que facilitan la circulación de la información – lo que podríamos definir como el entorno macro del ciberespacio – como los dispositivos que procesan, transmiten o almacenan la información que circula por el nivel macro – lo que podríamos definir como nivel meso – y finalmente el nivel micro, compuesto por el software y los datos intangibles generados por el mismo.

Los tres niveles del ciberespacio son vulnerables – no sólo por ataques intencionados, ya que la vulnerabilidad puede ser debida a desastres naturales – por lo cual es necesario establecer medidas de protección en todos los casos. Cada uno de ellos debe tener su propia estrategia de seguridad dependiendo de la criticidad de las vulnerabilidades y la gravedad de sus consecuencias.

Queda justificado, que el uso de Internet con fines terroristas como instrumento y/o medio para la comisión de sus actos es una realidad; Internet y las infraestructuras TIC como objetivo terrorista, es una hipótesis que cada vez toma más fuerza como una amenaza emergente.

El ciberespacio, plantea una serie de vulnerabilidades, que en el caso de las infraestructuras críticas son especialmente importantes. Los peligros principales son:

- La amplia interconexión entre las mismas, que genera múltiples dependencias entre ellas y la posibilidad de efectos en cascada.
- La posibilidad de convertirse en objetivos de ataque directo, o dentro de una acción concertada con un atentado convencional.
- La amplificación de los efectos psicológicos en la población que supondría un ataque de estas características por su repercusión en infraestructuras vitales para la población[27].

Otros factores tecnológicos que aumentan la posibilidad de ciberataques, son la complejidad y la rapidez de la evolución de la tecnología, que, a causa de las exigencias y competitividad del mercado, producen la puesta en funcionamiento de

[27] Encuentro Internacional de Seguridad de la Información T24; “Nuevas tendencias de ataque en Infraestructuras Críticas, enfoque desde las Fuerzas de Seguridad del Estado”; Jefatura de Información-Área Técnica de la Guardia Civil. https://www.incibe.es/enise2011/es/programa/dia-27/taller-24.html

productos con vulnerabilidades y fallos de seguridad, más difíciles de comprobar en los diseñados en países no occidentales, en los cuales es más problemático controlar la introducción de elementos inseguros.

No considerar la seguridad como un factor fundamental del diseño de productos o sistemas es otro factor de riesgo. España, fue el tercer país, tras Estados Unidos y el Reino Unido, que mayor número de ataques cibernéticos sufrió en 2014, según declaraciones del ministro de Asuntos Exteriores, con más de 70.000 ciberincidentes, de los que no detalló la gravedad[28].

En la presentación del nuevo Plan de Protección de las Infraestructuras Críticas el pasado 8 de marzo, el secretario de Estado de Seguridad, Francisco Martínez, facilitó los datos referidos a 2015, durante el cual, el CNPIC (Centro Nacional de Protección de Infraestructuras Críticas) resolvió alrededor de 50.000 incidentes, de los cuales 134 estaban dirigidos contra infraestructuras de este tipo. Adelantó que durante el presente año, la previsión de ciberataques ascendería a unos 100.000, de los cuales 300 serían contra dichas infraestructuras[29].

En este sentido, el director del CNPIC manifestaba que "hay que ser conscientes de que nos pueden hacer más daño con un ataque cibernético contra una infraestructura critica que con un atentado tradicional"[30].

Esto puede dar una idea de la gravedad de la amenaza terrorista utilizando técnicas de ciberterrorismo, ante la cual, tanto a nivel estatal, como de los Organismos Internacionales se están tomando de forma coordinada medidas tendentes a neutralizar el riesgo emergente que las ciberamenazas suponen para los estados miembros.

Para responder con la mayor rapidez posible a las ciberamenazas, y facilitar información preventiva sobre las mismas, se han creado distintos CERT[31] dependientes de organismos como el CCN (Centro Criptológico Nacional), CERTSI

[28] Información obtenida de http://politica.elpais.com/politica/2015/02/05/actualidad/1423136881_175042.html consultada el 1 de abril de 2016

[29] Información obtenida de http://www.interior.gob.es/es/web/interior/noticias/detalle/-/journal_content/56_INSTANCE_1YSSI3xiWuPH/10180/5721139/ consultada el 1 de abril de 2016

[30] Fernando Sánchez; Director del Centro Nacional de Protección de Infraestructuras Críticas; Diario ABC; 27-01-2015; http://www.abc.es/espana/20150127/abci-entrevista-ciberseguridad-201501271111.html

[31] Acrónimo de *Computer Emergency Response Team* es un centro de respuesta a incidentes de seguridad en tecnologías de la información.

(CERT de Seguridad e Industria), INCIBE (Instituto Nacional de Ciberseguridad) o REDIRIS (Red Española para la Interconexión de Recursos informáticos) que gestionan e investigan los posibles incidentes que afectan a la seguridad del ciberespacio y facilitan herramientas de eliminación de virus y consejos de seguridad para evitar vulnerabilidades de los equipos informáticos[32].

En el marco de la UE, el Centro Europeo de Cibercrimen (EC3), dependiente de Europol, se ocupa de los delitos relacionados con el ciberterrorismo, desde enero de 2013, centrándose principalmente en los delitos de fraude económico, los relacionados con ataques informáticos a empresas o infraestructuras críticas y explotación sexual infantil, así como a la recogida de información de inteligencia, de una gran variedad de fuentes tanto públicas como privadas a fin de alimentar una base de datos policiales, que permita facilitar información a los países miembros[33].

Durante quizá demasiado tiempo, no se consideró por las autoridades de los distintos estados occidentales, que la seguridad en la red podría ser un asunto estratégico. Una de las amenazas que se pueden dar en el tema de la seguridad, según Abraham R. Wagner es la de las organizaciones terroristas que están desarrollando capacidades de ciberguerra. Este autor, refiriéndose al caso de EE.UU. considera la década de los 90 del pasado siglo, como “la década pérdida” en materia de ciberseguridad[34].

En nuestro papel como “usuarios” en los distintos niveles del ciberespacio, los seres humanos somos los únicos responsables, hoy por hoy, de nuestros actos, en base a nuestra condición de seres “conscientes”. Aunque no hay un consenso acerca del significado del término consciencia, para Michio Kaku[35], se trata de una escala de tres niveles, en la cual el primero sería la capacidad de sentir y reconocer el entorno; el segundo sería la capacidad de ser autoconsciente, es decir tener desarrollado el sentido de quienes somos en relación con otros animales, otros seres humanos y el

[32] Para mayor información véase el siguiente enlace: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1483-ccn-cert-ia-0916-ciberamenazas-2015-tendencias-2016-resumen-ejecutivo/file.html

[33] Información obtenida de https://www.europol.europa.eu/ec3 consultada el 6 de marzo de 2016

[34] Wagner, Abraham; “La seguridad nacional estadounidense y las tecnologías de la información”; Revista Temas nº 81-82 Págs. 25-32; 2015; Traducción David González; Pág. 28

[35] Físico teórico de nacionalidad norteamericana y origen japonés, y uno de los creadores de la teoría de campos de cuerdas. Doctor en Física desde 1972, es titular de la cátedra Henry Semat de Física Teórica de la Universidad de Nueva York.

mundo, y por último la capacidad de planificar el futuro estableciendo objetivos y planes[36].

En base a nuestra consciencia, los resultados de nuestras acciones en el entorno cibernético reportaran beneficios o perjuicios. Potenciar los beneficios y minimizar los perjuicios es por lo tanto una tarea exclusiva de cada uno de nosotros dependiendo de nuestro papel.

Está claro que en todas las decisiones que tomemos, existe una dualidad entre las ventajas y los riesgos e inconvenientes de la misma. La complejidad del fenómeno de la globalización y el auge de las TIC, no es una excepción. Las ventajas de las mismas son patentes y considerables, pero los riesgos también existen y por lo tanto debemos tomar una serie de medidas para atenuarlos lo más posible.

La forma de conocer a nuestro enemigo que aconsejaba Sun Tzu sigue vigente en el fondo, pero ha cambiado radicalmente en la forma. La forma de vencerlo sigue igualmente vigente, Sun Tzu decía que la mejor forma de ganar la guerra era no tener que combatir. Hoy en día más que nunca, nuestra fortaleza y nuestra disuasión está en nuestra vigilancia.

Conclusiones

Estamos asistiendo a cambios profundos en nuestros hábitos. Estos cambios afectan a nuestra forma de comportamiento en muchos aspectos, sociales, laborales, económicos y personales. Nuestra vida se ha simplificado en lo que respecta a la realización de determinadas tareas que antes nos exigían un consumo de tiempo considerable, y ahora podemos realizarlas de forma instantánea.

Esta facilidad de realizar transacciones virtuales, nos ha hecho más vulnerables, especialmente en lo referente al aspecto social y económico. Una de las principales causas de esta relajación es la falsa sensación de seguridad que nos proporciona el anonimato con el cual tenemos la sensación de actuar cuando operamos a través de las TIC. El mismo anonimato con el que nosotros operamos, es utilizado por otros actores para atacar nuestros intereses como los de nuestras instituciones, las cuales

[36] Kaku, Michio; “La física del futuro;” Random House Mondadori, S.A.; Barcelona; 2º Edición; Enero 2012. Traducción de Mercedes García Garmilla. Págs. 144 y sig.

también están amenazadas. Esas amenazas pueden tener unas consecuencias importantes y, por lo tanto, debemos aprender a protegernos de ellas, en la medida de nuestras posibilidades.

En la adopción de estas medidas deben participar todos los actores que tienen algún tipo de intervención en el fenómeno, puesto que la colaboración entre ellos es imprescindible, en tanto que hemos sido los seres humanos los que hemos desarrollado el ciberespacio y sus infraestructuras, y somos los que las utilizamos.

Todos estos actores, tienen en común su condición de seres humanos. Por lo tanto, la primera conclusión sería que es el factor humano el principal responsable de las deficiencias del sistema, en función del papel que represente en el conjunto de las TIC[37]. El ciberespacio, sólo es un conjunto de medios técnicos y virtuales, pero son los fines con los que se utiliza los que definen la legitimidad de los resultados.

La mayoría utiliza los recursos de la red de forma legítima aprovechando las facilidades que esta ofrece para la realización de actividades como la información, el ocio, la educación, la realización de trámites diversos sin necesidad de desplazamientos, etc.

Este tipo de usuario es el eslabón más débil de la cadena de ciberseguridad. En este sentido es fundamental incrementar la formación y la sensibilización de los mismos a todos los niveles en el ámbito laboral y privado, a fin de que tomemos conciencia de los riesgos que implica la utilización de las tecnologías sin tener un adecuado conocimiento de las vulnerabilidades de las mismas y de los mecanismos de defensa y precaución a seguir en el uso de estas.

Medidas como el uso de la criptografía en las comunicaciones, la identificación en dos pasos, para el acceso a determinadas operativas, la instalación de antivirus eficaces, así como de las actualizaciones facilitadas por los desarrolladores de software, entre otras medidas, supondrían un importante incremento de la seguridad.

Los usuarios del ciberespacio con fines delictivos, en busca de un beneficio personal, por razones ideológicas, económicas o de cualquier otra índole, deben combatirse con

[37] A efectos del presente trabajo, he considerado tres distintos papeles: Usuarios, de los que formaríamos parte la mayoría de nosotros, independientemente de los objetivos con los que actuemos; dentro de los mismos, considero tres tipos de usuarios; los que acceden a los recursos con fines legítimos, los que lo hacen con fines delictivos en sentido amplio, y los que tienen tareas de vigilancia y seguridad. El segundo papel, sería el de los diseñadores de software, de sistemas principalmente, y por último el de los Administradores Públicos.

la coerción, dentro de los marcos de legalidad. Las últimas modificaciones legislativas llevadas a cabo tienen el objetivo de enmarcar las actuaciones de las fuerzas de seguridad, apoyándose en la ampliación de los delitos de terrorismo, en la prevención de la ciberdelincuencia.

Los diseñadores de sistemas e infraestructuras de seguridad, y desarrolladores de software y páginas web, deberían contar con una mayor dedicación de recursos tecnológicos y económicos al diseño y desarrollo de software de seguridad, paralela a una mayor exigencia de medidas de seguridad en el desarrollo de sistemas e ingeniería de software, que impidieran la toma de control de sistemas informáticos facilitados por vulnerabilidades de seguridad, como las conocidas como *backdoor*[38] entre otras.

La Administración Pública, además de la dotación de medios económicos y tecnológicos a la lucha contra las actividades de delincuencia, debería desarrollar medidas legislativas complementarias a las existentes – en el caso de España algunas de ellas de desarrollo reciente, como la modificación del Código Penal del pasado año[39] – aunque pudieran ocasionar fricciones entre los derechos fundamentales individuales y los colectivos, entre los cuales quizá el más conflictivo sería el derecho a la privacidad. Estos derechos, bajo garantía judicial, y en determinadas situaciones bajo amparo constitucional, pueden ser conculcados, y en beneficio del bien colectivo estarían justificados.

No se trata de retroceder en los hitos alcanzados en el Estado de Derecho, pero si convendría debatir sobre la importancia de los derechos individuales frente a los de la colectividad. En este sentido, el anonimato o la ocultación de la identidad (IP) en el acceso al ciberespacio debería restringirse, así como un mayor control de la denominada “Internet profunda”, lo que no tendría por qué suponer una disminución de derechos, ya que los usuarios que acceden a las redes con fines legítimos no ocultan

[38] Literalmente “puerta trasera”. Se trata de una vulnerabilidad en el software, que permitiría la toma de control del equipo o servidor de red donde se está ejecutando, abriendo la puerta en este último caso, a una infección masiva de los equipos conectados a ese servidor. No son necesariamente fallos de diseño, en algunos sistemas se codifican para permitir tareas de mantenimiento remoto silencioso. No obstante su utilización con fines criminales es un riesgo cierto y posible si no está debidamente asegurado o si los atacantes son capaces de burlar esta seguridad.

[39] Ley Orgánica 2/2015 del 30 de marzo de 2015 que reforma en su totalidad los artículos 571 a 580 del Código Penal, relativos a los delitos de terrorismo, en la que se introduce expresamente la configuración de los delitos informáticos como delitos de terrorismo cuando se cometan con finalidades terroristas.

su identidad, ni consideran una merma de derechos estar identificados. El simple hecho de saberse identificado, supondría una disminución de las acciones delictivas.

Debería existir una colaboración más estrecha con las empresas privadas, especialmente las dedicadas al desarrollo de nuevas tecnologías, especialmente aquellas que se desarrollan para las infraestructuras críticas, que como hemos visto pueden tener consecuencias importantísimas en el caso de sufrir un ataque de ciberterrorismo.

En este sentido, Abraham Wagner, considera que el gobierno no puede limitarse a legislar la seguridad[40], tiene que financiar su desarrollo y aplicación, y además debe contar con la colaboración de la industria dedicada al desarrollo de nuevas tecnologías[41].

Los cambios que estamos observando, no sólo afectan a nuestra forma de vida diaria. También están cambiando las maneras de dirimir conflictos entre Estados, y lo que es más preocupante: puede cambiar la forma de realizar atentados terroristas. Actualmente asistimos a ataques con armas y explosivos, cuyas consecuencias son evidentemente muy graves, pero pensemos en las consecuencias de la toma de control por una organización terrorista de una infraestructura crítica como una central nuclear o un dispositivo de control de armas atómicas. Podría darse el caso de que, en un futuro quizá demasiado próximo, esta hipótesis pueda convertirse en real y sus resultados podrían ser devastadores.

*Joaquín Ruiz Díaz***
Máster en Terrorismo-URJC

[40] Evidentemente se refiere a la ciberseguridad en concreto en este caso.

[41] Wagner, Abraham; “La seguridad nacional estadounidense y las tecnologías de la información”; Revista Temas nº 81-82 Págs. 25-32; 2015; Traducción David González; Pág. 31.