ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

02/2014 07 enero de 2014

Mª José Caro Bejarano

DELINCUENCIA ORGANIZADA E INTERNET. 2º parte.

DELINCUENCIA ORGANIZADA E INTERNET. 2º parte.

Resumen:

En un documento de análisis anterior se abordaba la preocupación por la delincuencia cibernética por parte de la industria y a los gobiernos. También se señalaba la necesidad de distinguir si un uso específico de delito organizado de Internet supone una amenaza para la seguridad nacional o internacional. Este documento continúa y termina de analizar esta cuestión que es primordial para encontrar las respuestas adecuadas.

Abstract:

A former analysis document addressed the concern about cyber crime by the industry and governments. It also noted the need to distinguish whether a specific use of the Internet organized crime poses a threat to national or international security. This document continues and finishes the analysis of this issue that is critical to find the right answers.

Palabras clave:

Ciberdelincuencia, Tecnologías de la Información y Comunicación, TIC, seguridad nacional e internacional, ciberamenazas, ciberataque, ciberseguridad, infraestructuras críticas.

Keywords:

Cyber-crime, Information and Communication Technology, ICT, national and international security, cyber threats, cyber-attack, cyber security, critical infrastructures.

DELINCUENCIA ORGANIZADA E INTERNET. Sus implicaciones para la seguridad nacional.

En un anterior documento se comenzaba el análisis sobre si un caso de ciberdelito organizado puede tener implicaciones para la seguridad nacional o internacional. Se señalaba la necesidad de distinguir qué actos ciberdelincuentes pertenecen a cada categoría para encontrar las respuestas adecuadas. En este documento se estudiarán estas cuestiones para intentar tener una visión clara y organizada de las mismas[1].

Un concepto problemático

El anonimato que ofrece Internet hace que sea relativamente fácil ocultar la identidad de uno y por lo tanto, a veces es difícil determinar si el autor del delito cibernético es un individuo, una organización o un agente de un tercer actor (ya sea estatal o no estatal).

Hackers expertos son capaces a menudo de evitar la atribución, que a su vez significa que los afectados por una intrusión en sus sistemas de información no pueden estar seguros de si el intruso es un actor solitario, un grupo delictivo organizado o un agente de un gobierno extranjero. De hecho, dos o más de estos supuestos pueden estar actuando conjuntamente, en virtud de acuerdos de patrocinio o alguna forma híbrida. Los grupos de la delincuencia organizada pueden adquirir código dañino especializado de un proveedor individual (se especula de forma considerable, por ejemplo, respecto al papel de un grupo de la delincuencia organizada conocido como el "Russian Business Network" en los ciberataques contra Estonia y Georgia y las relaciones de este grupo con el Kremlin en aquel momento[2]).

Tampoco se puede estar seguro de la ubicación física desde la que se origina el ataque. El ciberespacio no tiene fronteras y se puede cometer un delito contra un objetivo en el otro lado del mundo tan fácilmente como un objetivo en la propia jurisdicción. De hecho, una característica distintiva de la ciberdelincuencia es su naturaleza "sin fronteras", el delincuente, la víctima y la evidencia de un delito pueden cada uno estar localizados en diferentes ubicaciones físicas del mundo. Además, la mezcla de lo público y privado en las sociedades industriales avanzadas significa que el espacio de la ciberdelincuencia es de gran fluidez. En un día, un ciberdelincuente profesional puede estar trabajando para un gobierno, al día siguiente, para sí mismo, y el día después para una organización delictiva.

Por ello, la definición estándar de la delincuencia organizada, basada en tres o más personas que actúen conjuntamente impulsadas por el afán de lucro, puede no reflejar con precisión las complejidades y peculiaridades de su encarnación en el ciberespacio. Por ejemplo, no

[1] Grabosky, Peter, *Organised Crime and the Internet*, The RUSI Journal, 2013.
[2] Korns, Stephen W. y Kastenberg, Joshua E., *Georgia's Cyber Left Hook*, disponible en http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/08winter/korns.pdf

incluye ciertas formas de organización muy sofisticadas, tales como la movilización de botnets (abreviatura de redes de robots en inglés, nets of robots), que es considerada por algunos analistas como una forma de actividad delictiva organizada. Las botnets implican un delincuente, que a menudo actúa solo, que usa código dañino para adquirir el control de un gran número de equipos (puede alcanzar incluso más de un millón de máquinas separadas).

Los propietarios o gestores individuales e institucionales de ordenadores comprometidos, de esta manera, pueden ser partícipes involuntarios en una empresa delictiva, sin embargo, esta forma diferente de organización, gracias a la tecnología, permite a un individuo o a un pequeño número de personas, acceder sin permiso, y controlar, activos personales de la empresa y potencialmente una vasta cantidad de información.

Los múltiples usos delictivos de Internet

A un nivel muy básico, los delincuentes utilizan Internet para sus actividades de la misma forma que los demás individuos: como medio de comunicación o como un medio de almacenamiento de registros u otra información. Los fabricantes de drogas ilícitas, por ejemplo, comercian con recetas a través de Internet. Esta es la primera de las tres formas en que los delincuentes utilizan Internet: como instrumento del delito. Sin embargo, y quizás más importante, también puede servir como objetivo de la delincuencia e incluso como apoyo incidental de la actividad delictiva. Los tres modos se aplican a su uso individual y organizacional, y no son mutuamente excluyentes.

De manera común, Internet se usa como instrumento para atacar a otros sistemas informáticos. La mayoría de los ciberdelitos comienzan cuando un delincuente obtiene acceso no autorizado a otro sistema. Los sistemas son atacados a menudo con el fin de destruir o dañarlos a ellos y a la información que contienen. Esto puede ser un acto de vandalismo o protesta, o una actividad realizada en cumplimiento de otros objetivos políticos. Una de las formas más comunes es la denegación distribuida de servicio (DDoS), que implica la inundación de un sistema informático con un volumen masivo de información para que el sistema se ralentice significativamente. Las botnets son muy útiles para tales fines, ya que realizan múltiples solicitudes de servicio coordinadas.

Un ejemplo conocido de ataque DDoS iniciado mediante botnet se produjo en abril de 2007, cuando los servidores públicos y comerciales de Estonia se vieron seriamente degradados durante varios días. Los servicios bancarios en línea se vieron interrumpidos intermitentemente, y se limitó el acceso en línea a los sitios del gobierno y de los medios de comunicación. Según algunas fuentes los ataques tuvieron su origen en Rusia[3] y se alegó

[3] Landler, Mark y Markoff, John, *Digital Fears Emerge After Data Siege in Estonia,* *New York Times*, 29 de mayo

que fue el resultado de la colaboración de organizaciones juveniles rusas y grupos del crimen organizado ruso, tolerada por el Estado, aunque el grado en que supuestamente el gobierno ruso fue cómplice en los ataques no estuvo claro.

Al igual que los actores estatales o sus agentes pueden usar Internet para perseguir lo que ellos perciben como objetivos de la seguridad nacional, los grupos insurgentes y extremistas utilizan la tecnología de Internet de diversas maneras para promover sus causas. Estas incluyen el uso de Internet como instrumento de robo para aumentar su base de recursos; por ejemplo, como un vehículo para el fraude.

Sin embargo, Internet no se utiliza para fines ilícitos exclusiva o principalmente por los actores políticos. Los grupos de la delincuencia organizada la utilizan a diario a una escala global, con la participación en actividades que van desde la adquisición ilícita, la copia y la difusión de propiedad intelectual (la piratería supuestamente ha costado a las industrias de software y entretenimiento miles de millones de dólares[4]), al saqueo de datos de banca y de tarjetas de crédito, de secretos comerciales e información clasificada en poder de los gobiernos. Esto también puede comenzar con el acceso no autorizado a un sistema informático: de hecho, el robo de datos personales financieros ha servido de base para un mercado floreciente de estos datos, que permite el fraude a una escala importante.

La ciberdelincuencia organizada como una amenaza a la seguridad

La tecnología digital se ha generalizado y como resultado, la vulnerabilidad frente a la ciberdelincuencia ha aumentado proporcionalmente. Si uno contempla algunas de las formas que la ciberdelincuencia ha tomado en los últimos años, puede reconocer fácilmente el riesgo potencial para la seguridad nacional.

El ejemplo anterior del ataque a los servidores del gobierno de Estonia destaca el vínculo entre el ciberdelito organizado y la seguridad, y plantea la cuestión de si ciertos tipos de delitos cibernéticos, llevados a cabo con el patrocinio del Estado o por agentes del Estado, pueden considerarse actos de guerra. Tradicionalmente, un acto de guerra supone la amenaza de o el uso de la fuerza por un Estado contra la integridad territorial o la independencia política de otro. La ciber-actividad ha introducido una nueva variable en la ecuación, lo que requiere una nueva definición de lo que constituye un acto de hostilidad

---

de 2007. Véase en http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all

[4] En la actualidad no existen estimaciones fiables del coste de la ciberdelincuencia organizada. Un informe de Dettica de 2011 valoraba el coste en 27.000 millones de libras esterlinas en el Reino Unido que supone un 2% del PIB de este país. Un posterior estudio de 2012 lo situaba en el 5% del PIB de ese país, Anderson et al., *Measuring the cost of cybercrime*.
Disponible en: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

entre los Estados y cómo debe ser entendida en términos legales. Una vez más, un ejemplo bien conocido se desarrolló en 2010, cuando se hizo evidente que los sistemas de control que soportaban el programa de enriquecimiento de uranio del gobierno iraní habían sido infectados por un código dañino y que, en consecuencia, se habían destruido un número considerable de centrifugadoras[5].

Además, las aplicaciones militares de las tecnologías de Internet se han discutido abiertamente por lo menos desde 1998.Desde entonces, la militarización del ciberespacio ha continuado a buen ritmo. Un número desconocido de naciones están desarrollando capacidades ofensivas de guerra cibernética o ciberguerra, que podría, entre otras cosas, interferir con los sistemas de mando, control y comunicaciones, y perturbar o destruir infraestructuras críticas. Ya en octubre de 2012, el Secretario de Defensa de EE.UU., Leon Panetta habló de un "ciber -Pearl Harbor" en manos de un Estado hostil o un grupo extremista[6].

Los Estados y los actores no estatales se dedican al ciberespionaje - se estimó ya en 2007 que más de 100 países de todo el mundo participaban en alguna forma de esta actividad[7]. La prevalencia es poco probable que haya disminuido desde entonces, como sugieren los titulares de los últimos meses.

La vulnerabilidad de los secretos gubernamentales ante el robo (a pesar de la tendencia de algunos guardianes de estos secretos para exagerar su valor) se ilustró más claramente con la publicación de unos 400.000 cables diplomáticos del Departamento de Estado de EE.UU. por la organización Wikileaks. Es poco probable que la copia y amplia difusión de tal gran cantidad de información hubiera ocurrido sin la concurrencia de la tecnología digital. Algunos podrían argumentar que la revelación de información clasificada es, ipso facto, una amenaza para la seguridad nacional, mientras que otros pueden sostener que el acto de clasificación de la información es subjetivo en sí mismo y que la transparencia debe prevalecer.

---

[5] David Alandete, El País, 1-6-2012: El New York Times reveló la existencia de un programa de ciberataques, bautizado por la Administración de George W. Bush como operación Juegos Olímpicos. Se detalla además en un libro titulado 'Confrontación y ocultación: las guerras secretas y el sorprendente uso del poder americano de Obama', del escritor David Sanger.
Véase en http://internacional.elpais.com/internacional/2012/06/01/actualidad/1338572841_317814.html

[6] El País 12 de octubre de 2012, El Secretario de Defensa de EE.UU avisa del riesgo de un ataque cibernético. Véase en: http://internacional.elpais.com/internacional/2012/10/12/actualidad/1350061446_784106.html

[7] Brodkin, Jon, *Government-Sponsored Cyberattacks on the Rise, McAfee Says*, Network World, 29 de noviembre de 2007. Véase en http://www.networkworld.com/news/2007/112907-government-cyberattacks.html?page=1

Este ejemplo también pone de relieve lo difícil que es definir la ciberdelincuencia organizada en determinadas circunstancias: Wikileaks es una organización que no puede ser clasificada como un grupo de delincuencia organizada bajo cualquier definición tradicional, en lo que respecta a la actividad criminal organizada en Internet, con repercusiones en seguridad, toda categorización buena es difícil de alcanzar. También apunta a otro nivel de complejidad: los grupos no estatales y los particulares, cuando actúan sin el patrocinio del Estado, tienen igualmente la capacidad para interrumpir y por lo tanto, de amenazar la seguridad nacional. La interrupción, por ejemplo, del comercio electrónico y los servicios bancarios pondría en peligro una de las principales plataformas de desarrollo económico.

La diversidad del Delito Cibernético Organizado

A continuación se recoge una breve reseña descriptiva de la actividad ciber-criminal específica atribuida a las organizaciones. Los ejemplos seleccionados, sin ser representativos del universo de la ciberdelincuencia organizada, son ilustrativos de la gran diversidad de actividades de delincuencia organizada que es dependiente de Internet, sus repercusiones sobre la seguridad, y los motivos de aquellos que emprenden tal actividad. Esto puede de alguna manera resaltar lo difícil que todavía puede ser compartimentar claramente los diferentes tipos de comportamiento delictivo organizado en línea.

La productora Azov Films, con sede en Toronto, y su propietario, Brian Way, fueron los principales objetivos de la operación *Proyecto Espada* que permitió desmantelar una extensa red de pornografía infantil. La empresa aparentemente se dedicaba a la distribución de DVD y películas en *streaming* de carácter naturista, legales en Canadá y EE UU, pero, bajo esa tapadera, Way enviaba vídeos con imágenes de menores desnudos a 94 países, obteniendo unos ingresos anuales de 1.600 millones de dólares. Esta operación policial, con origen en Canadá, y con ramificaciones en, entre otros países, España, Irlanda, Suecia, Noruega, Sudáfrica, Australia, Estados Unidos, México o Hong Kong, se saldó con 340 detenidos en varios países, incluida España. La investigación, se inició en 2010, se han incautado hasta 45 terabites que almacenaban cientos de miles de fotografías e imágenes sexuales de menores.

El grupo Anonymous es un colectivo flexible de anarquistas basado en gran parte en valores compartidos de travesuras y el resentimiento frente a la autoridad, que se dedican a lo que se ha denominado “hacktivismo” o activismo en la red. El valor dominante de la iconoclastia comenzó a centrarse en símbolos importantes. Los métodos elegidos son desfiguraciones de sitios web y los ataques DDoS, complementados por el abuso verbal en la red. No en vano, la página web de la Agencia Central de Inteligencia de EE.UU. (CIA) representó un objetivo atractivo. Imbuido del espíritu hacker de que la información debe ser libre, el grupo también

se dirigió al secreto de la Iglesia de la Cienciología, la comercializadora en exclusiva de la Asociación Cinematográfica de EE.UU., y se convirtió en un partidario de Wikileaks.

Cuando el gobierno de EE.UU. convenció a varios proveedores de servicios electrónicos de pago de suspender el procesamiento de las contribuciones a Wikileaks, Anonymous orquestó ataques DDoS contra los que lo cumplieron.

El virus ZeuS fue refinado por ingenieros de software de Europa del Este y fue identificado por primera vez en julio de 2007, y se extendió de forma más generalizada en la primavera de 2009. Este código dañino fue utilizado por piratas informáticos ucranianos para obtener acceso a los ordenadores de personas empleadas en una variedad de pequeñas empresas, municipios y organizaciones no gubernamentales en EE.UU. Se desarrolló una plaga virtual con un simple y peligroso objetivo: robar contraseñas y datos de las cuentas bancarias de sus víctimas. Los equipos destino se veían comprometidos cuando la víctima abría un mensaje de correo electrónico aparentemente benigno. Con el acceso a los detalles de la cuenta bancaria y la contraseña de las víctimas, los atacantes de Ucrania fueron capaces de iniciar sesión en los organismos objetivo de las cuentas bancarias. Los cómplices de los atacantes de Ucrania colocaron anuncios en idioma ruso en sitios web invitando a estudiantes residentes en EE.UU. a ayudar en la transferencia de fondos fuera del país. A estos denominados "mulas" se les proporcionaron pasaportes falsificados y fueron dirigidos a abrir cuentas con nombres falsos en diversas instituciones financieras de EE.UU. Después de haber transferido los fondos obtenidos ilícitamente a las cuentas de las mulas, los atacantes instruyeron a las mulas para mover los fondos a cuentas en el extranjero o, en algunos casos, en el contrabando de los fondos físicamente fuera de EE.UU.

En Facebook reapareció este año con una nueva estrategia: utiliza Facebook para infectar ordenadores. El virus provoca que el ordenador del usuario no se apague una vez activado. Según algunos informes, el virus se adjunta en enlaces falsos de Facebook y cuando se entra en el vínculo, el usuario es redireccionado a una página pidiendo que se descargue un software común. Tras ser descargado el virus se activa. A partir de ese momento, cada vez que un usuario acceda a sus cuentas bancarias, está en peligro. Zeus, también conocido como ZBOT, es tan poderoso que puede incluso sustituir a la página principal de la institución financiera con el fin de engañar a la gente para que entregue sus datos.

La Policía Nacional detuvo en mayo de este año a los responsables de un grupo que defraudó en Internet más de 750.000 euros con tarjetas clonadas. Los detenidos presuntamente formarían la cúpula directiva de la organización en nuestro país. Compraban en la Red productos electrónicos de alta gama con tarjetas de crédito fraudulentas para, posteriormente, venderlos en páginas web de compraventa sirviéndose de empresas

pantalla. Se les imputaron delitos de falsificación de documento mercantil, blanqueo de capitales, pertenencia a organización criminal, estafa informática y alzamiento de bienes. Obtenían los datos de las tarjetas mediante troyanos, phishing o pharming[8].

La operación Juegos Olímpicos (Olympic Games) era una colaboración entre la Agencia Nacional de Seguridad de EE.UU. (NSA) y su homólogo israelí, Unidad 8200, con la intención de interrumpir el programa de enriquecimiento de uranio iraní[9]. Presuntamente implicó la inserción clandestina de un software extremadamente complejo y sofisticado (comúnmente conocido como Stuxnet) en los sistemas de comunicaciones y control en las instalaciones nucleares de Natanz. El software incluía la capacidad para supervisar las comunicaciones y la actividad de funcionamiento, así como la capacidad de corromper los sistemas de control de la instalación. La operación tuvo éxito al retrasar el progreso de enriquecimiento de uranio a través de la destrucción por control remoto de un número de centrifugadoras utilizadas en el proceso. El secreto que rodeó la operación se comprometió, en parte, cuando el código dañino saltó a Internet debido a un error de programación. Esta operación es la ciber-operación conjunta más conocida hasta ahora[10].

GhostNet fue el nombre dado por un grupo de investigadores canadienses en 2010 a una operación de ciberespionaje que, al parecer, operaba desde cuentas comerciales de Internet en China. Los hackers comprometieron los ordenadores del gobierno en más de 100 países, también dirigieron correos electrónicos enviados a través del servidor del Dalai Lama. El gobierno chino negó su participación directa y no hubo pruebas concluyentes de lo contrario. Hay, sin embargo, alguna evidencia de la complicidad del gobierno. A disidentes que regresaron a China desde el extranjero, las autoridades chinas les mostraron las transcripciones de chats de internet en el que estaban implicados esos disidentes mientras estaban fuera del país. Por lo menos, esto sugeriría que el gobierno era encubridor[11].

Quizás uno de los grupos más conocidos que participaba en la ciberdelincuencia organizada (en este caso, supuestamente, patrocinado por el Estado) es la Unidad 61.398 del Ejército Popular Chino (People Liberation's Army, PLA). En febrero de 2013, la empresa estadounidense de seguridad de la información Mandiant informó sobre un programa a gran escala de espionaje industrial que había comenzado en 2006 en la Unidad

[8] Más información en http://www.policia.es/prensa/20130521_1.html
[9] Esta operación se detalla en el libro titulado *Confront and Conceal*, de David Sanger.
[10] Sanger, David E. y Shanker, Thom. *Obama to Keep Security Agency and Cyberwarfare Under a Single Commander*, The New York Times, 13 de diciembre de 2013, Véase en: http://www.nytimes.com/2013/12/14/us/politics/obama-to-keep-security-agency-and-cyberwarfare-under-a-single-commander.html?_r=0
[11] *Tracking GhostNet: Investigating a Cyber Espionage Network,* 29 de marzo de 2009,Véase en: http://www.securityfocus.com/blogs/1809

mencionada[12]. Con sede en Shanghai, esta organización se hizo supuestamente con un volumen masivo de datos de una amplia variedad de industrias en los países de habla inglesa. La información presuntamente extraída incluye especificaciones técnicas, estrategias de negociación, documentos de precios y otros datos propietarios. Uno de los objetivos supuestos, un importante fabricante de bebidas EE.UU., estaba planeando en 2009 lo que iba a ser hasta la fecha, la mayor adquisición extranjera de una empresa china. Un aparentemente inocuo e -mail a un ejecutivo de la compañía estadounidense contenía un enlace que, al abrirse, permitía a los atacantes acceder a la red de la empresa. Según el informe de Mandiant, intrusos chinos accedieron regularmente a información sensible sobre las negociaciones pendientes, y finalmente la compra no se hizo realidad. No está claro si la unidad del PLA está formada exclusivamente por personal militar o incluye contratistas civiles.

La NSA, National Security Agency, parte del Departamento de Defensa de EE.UU desarrolla un programa a gran escala de captura, almacenamiento y análisis de datos desde 2001. Este programa divulgado por Edward Snowden, exanalista subcontratado de la NSA, se ha basado en gran medida en la cooperación de los operadores de telecomunicaciones y los proveedores de servicios del sector privado y a la participación de consultores privados contratados, de los cuales Snowden fue uno. Las empresas que cooperaron son conocidas en el ámbito de Internet. El programa, según se informó, capturó y almacenó una amplia variedad de datos, incluyendo mensajes de correo electrónico, intercambio de chats, voz sobre protocolos de Internet (VoIP), fotografías, datos, transferencia de ficheros, videoconferencias y otros contenidos de redes sociales. La NSA y sus socios del sector privado también lograron eludir las tecnologías de cifrado en la red. Se dio a conocer, entre otras cosas, que se interceptaron las comunicaciones, entre otros, de los presidentes de Brasil y México, el Ministerio de Relaciones Exteriores de Francia, y Petrobras, la compañía petrolera paraestatal brasileña[13].

Los ejemplos anteriores de ciberdelincuencia organizada sugieren que no todas las organizaciones que actúan ilegalmente en el ciberespacio pueden ser consideradas como una amenaza para la seguridad nacional o internacional. Alguna actividad es, sin duda molesta, ofensiva en extremo, y a menudo dañina. Mientras tanto, hay algunas actividades en línea que, podrían posiblemente debilitar la integridad y la economía de los Estados, y por

[12] *Mandiant Intelligence Center Report, APT1: Exposing One of China's Cyber Espionage Units*. Disponible en: http://intelreport.mandiant.com/.

[13] Greenwald, Glenn, XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet", Guardian, 31 de julio de 2013. Véase en http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data; Saiz, Eva, *EE.UU. accede a información de usuarios de los gigantes de internet,* El País, 7 de junio de 2013.
Véase en http://internacional.elpais.com/internacional/2013/06/07/actualidad/1370564066_752776.html.

lo tanto llegar a ser considerados como amenazas a la seguridad. Las industrias de software y entretenimiento de EE.UU. argumentan que la piratería cuesta a la economía doméstica millones de dólares en ganancias perdidas, y tiene un efecto amedrentador sobre el espíritu emprendedor y la creatividad en todo el mundo. Sin embargo, la economía de EE.UU. es lo suficientemente variada que la fortaleza de su futuro dependerá de otros factores.

De hecho, se podría argumentar que la piratería permite que los ciudadanos de los países menos desarrollados se beneficien del acceso a productos que de otra manera no podrían permitirse. Del mismo modo, hay quienes argumentan que organizaciones como Wikileaks, de hecho, proporcionan un servicio liberando información que no debería ocultarse al público. Por otro lado, el principal y persistente espionaje industrial y político, en una escala más amplia puede también poner en peligro la seguridad del Estado.

El espionaje industrial puede debilitar la competitividad internacional de una empresa o de un sector industrial, en el caso más obvio, cuando la información en cuestión se refiere a los sistemas de armas. Del mismo modo, el robo de datos bancarios y de tarjetas de crédito, si ocurriera a una escala más grande, sin duda dificultaría la actividad comercial, con el correspondiente daño a la economía de un Estado. Por el momento, sin embargo, los bancos absorben las pérdidas (o las pasan al consumidor) y el fraude en línea parece tolerable. La seguridad de las tecnologías de la información necesita refinarse y los conocedores de la tecnología, al menos en los países desarrollados, son, en su mayor parte, capaces de protegerse a sí mismos. La banca on-line y el comercio electrónico también continúan prosperando. En los países menos desarrollados, sin embargo, donde los usuarios acaban de entrar en la era digital, la falta de conciencia de ciberseguridad puede aumentar la vulnerabilidad de los individuos y de las organizaciones de los sectores público y privado. En la medida en que la amenaza de la ciberdelincuencia impide el desarrollo del comercio electrónico, podría contribuir al debilitamiento de la seguridad económica de una nación.

En lo que se refiere a las organizaciones, se observa que las mayores amenazas a la seguridad nacional son planteadas por los propios Estados, ya sea sin ayuda o con la colaboración de aficionados expertos o sofisticados ciberdelincuentes. La actividad cibernética que condujo a la destrucción de las centrifugadoras iraníes sería sin duda definida por las autoridades de ese país como una amenaza a su seguridad. Las naciones que han recibido ataques similares podrían inclinarse a considerarlos como actos de ciberguerra.

Mientras tanto, las actividades de Anonymous, como espiar una conferencia telefónica entre los agentes del orden público y los intentos de cerrar la página web de la Agencia Central de Inteligencia (CIA), han sido ciertamente molestas para las autoridades de Estados Unidos. Aunque embarazosa, esta actividad a escala relativamente baja no constituye daño a la

seguridad nacional. Sin embargo, si se realiza persistentemente o a una escala más grande, tal actividad puede enviar un mensaje de indiferencia por parte del Estado, en el mejor de los casos, y de incompetencia, en el peor de ellos, y por lo tanto, invitar a la imitación por parte de muchos otros atacantes. El potencial de un daño importante, por tanto, es real. El umbral de la amenaza a un objetivo parece ser una función del alcance y la intensidad de la actividad criminal, por una parte, y la capacidad de resistencia y recuperación del Estado y de su infraestructura en el otro.

En el caso de Wikileaks, sus declaraciones pueden haber dificultado la capacidad de los diplomáticos de EE.UU. para obtener comentarios sinceros de informantes locales en todo el mundo. Algunas de estas revelaciones parecen haber aumentado la vulnerabilidad de los regímenes débiles y, a tal fin, la ciberdelincuencia organizada era, sin duda, una amenaza a su seguridad. Si esto va a mejorar o interferir con la seguridad de EE.UU. aún está por verse.

CONCLUSIÓN

Si la delincuencia cibernética o ciberdelito organizado se produjera a una escala mayor, podría dar lugar a un debilitamiento de la confianza en las principales instituciones públicas o privadas. La cuestión fundamental es en qué momento la naturaleza y la escala de la ciberactividad criminal (organizada o no) comienza a constituir una amenaza a la seguridad. La cuestión no es si una nación es segura o no, sino si una circunstancia específica puede contribuir a una mejora o disminución de la seguridad.

Cabe destacar en este sentido que muchos de esos delincuentes que operan actualmente en el ciberespacio, solo o dentro de las organizaciones, eran técnicos competentes antes de dedicarse a la delincuencia. Lo que es interesante es el papel relativamente menor que los grupos delictivos organizados convencionales han jugado hasta ahora en la ciberdelincuencia. El uso principal de la tecnología de Internet parece haber sido accidental, como medio de comunicación y del mantenimiento de registros.

Hay ejemplos de organizaciones delictivas convencionales en que participan especialistas en Tecnologías de la Información para tareas específicas. (Este modelo de compromiso no es diferente a la de los traficantes de drogas a gran escala que contratan a profesionales químicos para ayudarles en el perfeccionamiento de la heroína o la fabricación de drogas sintéticas.)

Mientras tanto, la tecnología digital con aplicación criminal directa es cada vez más sofisticada y más accesible. Los piratas informáticos a sueldo abundan en el ciberespacio. El potencial de los kits de código dañino o “exploits” para ser utilizados o vendidos en el mercado por las organizaciones delictivas ya es importante y es probable que aumente. No

sólo se pueden alquilar estos kits; los arrendadores también ofrecen apoyo a los usuarios, y pueden proporcionar también actualizaciones regulares como parte del acuerdo de servicio. No cabe duda de que los delincuentes organizados convencionales que han crecido en la era digital abrazarán la tecnología como una cuestión rutinaria, si no lo han hecho ya, tanto para fines mundanos como ilícitos.

Dada la omnipresencia actual de la tecnología digital, su accesibilidad por las organizaciones delictivas y su evidente utilidad para una variedad de fines delictivos, no hay duda de que la amenaza potencial a la seguridad nacional e internacional se mantendrá y, de hecho, se intensificará.

La preocupación por la vulnerabilidad en el ámbito digital explica ciberseguridad que países del mundo desarrollado y organizaciones internacionales hayan desarrollado estrategias de ciberseguridad en sus legislaciones. En el caso español, se ha unido a este conjunto de países con la aprobación el pasado cinco de diciembre de la Estrategia de Ciberseguridad Nacional[14], que viene a tratar de un modo más detallado el ámbito de la ciberseguridad ya contemplado en la Estrategia de Seguridad Nacional aprobada en mayo de este año[15].

Mª José Caro Bejarano
Analista Principal IEEE

[14] La Estrategia de Ciberseguridad se puede consultar en la siguiente dirección: http://www.lamoncloa.gob.es/NR/rdonlyres/680D00B8-45FA-4264-9779-1E69D4FEF99D/255433/20131332_completo_05dic13_0955h.pdf.

[15] La Estrategia de Seguridad Nacional se puede consultar en la siguiente dirección: http://www.lamoncloa.gob.es/NR/rdonlyres/0BB61AA9-97E5-46DA-A53E-DB7F24D5887D/0/Seguridad_1406connavegacionfinalaccesiblebpdf.pdf.