AMERICANA

Boletín Informativo de la Embajada de los Estados Unidos - Panamá Mayo 2006

Delitos Electrónicos

Sección Informativa y Cultural
Centro de Recursos Informativos
Amador Washington
Edificio Clayton, Clayton
Tel: 207-7100 / Fax: 207-7363

La lucha contra el delito en línea electrónica

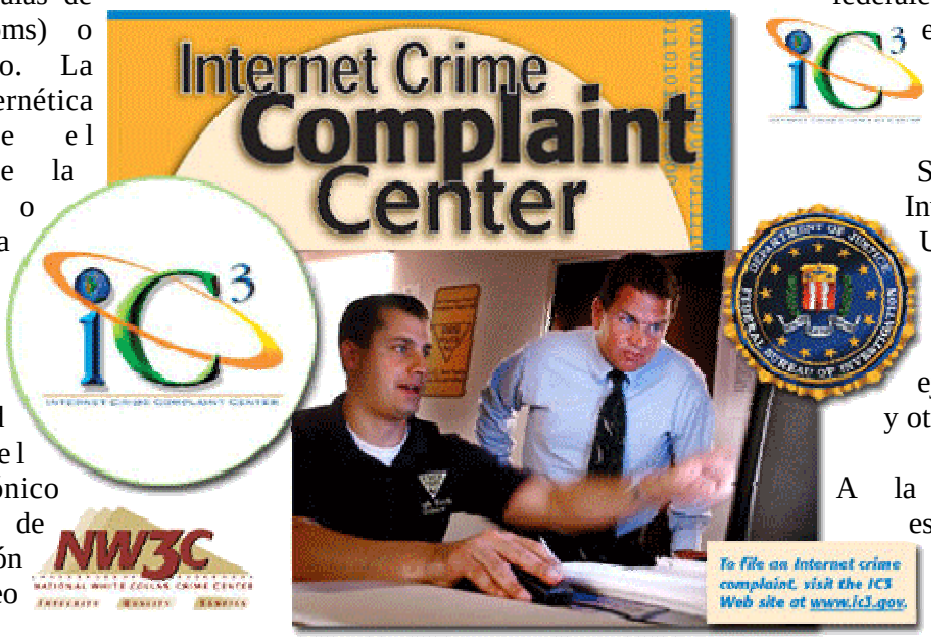
Por Daniel Larkin

Con el comercio en línea electrónica ha hecho su aparición la delincuencia en línea. Los organismos encargados de la ejecución de la ley han ideado nuevos métodos y establecido nuevas relaciones para atrapar a los delincuentes que actúan en el espacio cibernético.

Daniel Larkin es jefe del Centro de Denuncias de Delitos en Internet) (IC3) en la Oficina Federal de Investigaciones (FBI).

El Centro de Denuncias de Delitos en Internet (IC3) es un servicio de tramitación y remisión de denuncias presentadas por individuos en Estados Unidos y en todo el mundo. Mediante un formulario de presentación de denuncias en línea y un equipo de agentes y analistas, el IC3 sirve al público y a los organismos internacionales de ejecución de la ley que investigan la delincuencia en Internet.

La delincuencia en Internet, también llamada delincuencia cibernética, es toda actividad ilícita derivada de uno o más componentes de Internet, como sitios en la web, salas de tertulia (chat rooms) o correo electrónico. La delincuencia cibernética abarca desde el incumplimiento de la entrega de bienes o servicios y la intrusión en ordenadores, al uso indebido del derecho de propiedad intelectual, el espionaje electrónico (robo o comercio de secretos), la extorsión en línea, el blanqueo internacional de dinero, el robo de identidad y una lista cada vez mayor de otros delitos facilitados por Internet.



Fotomontaje: El Internet Crime Complaint Center del FBI (IC3) es un centro de coordinación de denuncias individuales de actividades delictivas en línea. El IC3 correlaciona la información de, tal vez, centenares de víctimas del mismo tipo de fraude y establece un caso importante, de cuyo procesamiento se encargarán los organismos de ejecución de la ley (Foto de AP/Wide World Photos: Logotipo facilitado amablemente por el Internet Crime Complaint Center).

La delincuencia hace su aparición en línea

El concepto del IC3 surgió en 1998 con el reconocimiento de que la delincuencia estaba introduciéndose en Internet porque los negocios se estaban realizando a través de este medio, y el consiguiente interés del FBI en seguir la pista de esas actividades delictivas y elaborar técnicas de investigación concebidas específicamente para combatir los delitos cometidos a través de Internet.

En aquel tiempo, no existía ningún lugar donde se pudieran denunciar los delitos cometidos a través de Internet, y el FBI deseaba distinguir la delincuencia en línea de otras actividades delictivas que se denuncian normalmente a la policía, al FBI y a otros organismos federales encargados de la ejecución de la ley, la Comisión Federal de Comercio, el Servicio de Investigación Postal - USPIS - (dependencia del Servicio Postal encargada de la ejecución de la ley), y otros.

A la primera oficina, establecida en 1999 en Morgantown, Virginia Occidental, se le dio el nombre de Centro de Denuncias de Fraude en Internet. Era una asociación del FBI y el Centro Nacional contra la Delincuencia de Guante Blanco, contratista sin fines de lucro del Departamento de Justicia, cuya misión principal es mejorar la capacidad de los agentes estatales y locales encargados de la ejecución de la ley

de detectar y responder a la delincuencia en los sectores económico y cibernético.

En 2002, para esclarecer el alcance de la delincuencia cibernética que se estaba analizando, de simple fraude a la gama de actividades delictivas que estaban apareciendo en línea, el centro cambió su nombre a Internet Crime Complaint Center y el FBI invitó a otras agencias federales (USPIS, la Comisión Federal de Comercio, el Servicio Secreto y otros), a ayudar a dotar de personal al centro y a contribuir a la labor contra la delincuencia el línea.

Hoy, en el IC3 de Fairmont, Virginia Occidental, seis agentes federales y unos 40 analistas de la industria y de instituciones académicas reciben denuncias de delitos cometidos a través de Internet presentadas por el público, denuncias que tramitan y posteriormente cursan a organismos federales, estatales, locales e internacionales de ejecución de la ley o agencias reguladoras y grupos especiales integrados por personal de múltiples instituciones, para su investigación.

En el sitio del IC3 en la web (http://www.ic3.gov), individuos de todo el mundo pueden presentar denuncias de delitos cometidos a través de Internet. En el sitio de la web se pide el nombre, la dirección y el número de teléfono del denunciante; el nombre, la dirección y el número de teléfono y la dirección en la web, en su caso, de la persona u organización de la que se sospecha que es responsable de alguna actividad delictiva; detalles de cómo, por qué y cuándo se cree que una persona ha cometido un delito y cualquier otra información que respalde la denuncia.

Cómo se establece un caso

El principal objetivo operativo del IC3 es recibir la denuncia de un ciudadano particular que pueda representar un delito causante de daños por valor de, digamos, 100 dólares, y combinarlo con información de otras 100 o 1.000 víctimas de todo el mundo que han perdido dinero por la misma estratagema, y establecer un caso importante a la mayor brevedad.

En realidad, la mayor parte de las agencias de ejecución de la ley no están autorizadas a investigar casos que entrañen cantidades relativamente pequeñas de dinero —100 dólares es probablemente una cantidad inferior a la que puede dar lugar a una investigación. Pero la mayor parte de los delincuentes están en línea para ampliar el alcance de sus oportunidades de hacer víctimas y obtener dinero; un delito cibernético casi nunca tiene una sola víctima. Así pues, los investigadores del IC3 pueden vincular denuncias afines y transformarlas en un caso de 10.000 ó 100.000 dólares, con 100 ó 1.000 víctimas; entonces el delito pasa a ser un asunto importante y las agencias de ejecución de la ley lo pueden investigar.

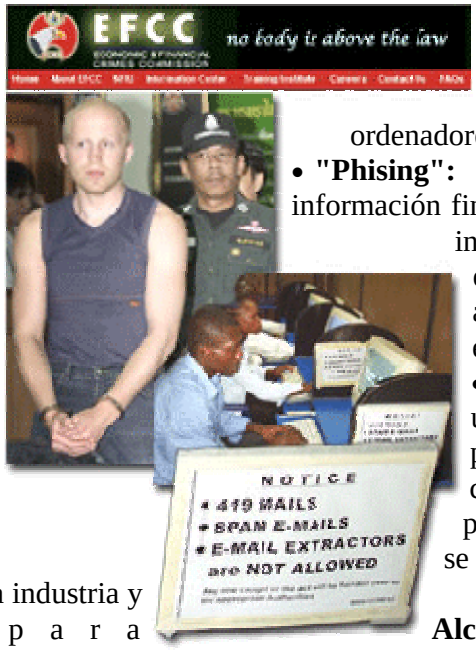
El IC3 a veces ayuda a las agencias de ejecución de la ley con la investigación y el establecimiento del caso inicial. En los primeros dos años y medio del proyecto, pese a un intento de establecer casos y cursarlos rápidamente a las agencias de ejecución de la ley, el IC3 pudo comprobar que no todos los grupos especiales encargados de la lucha contra la delincuencia cibernética estaban equipados para rastrear o investigar rápidamente los delitos relacionados con Internet. Algunos grupos especiales pueden carecer de los medios de llevar a cabo una operación clandestina o de seguir el rastro digital de las pruebas que les transmite el IC3, por lo que es importante que el IC3 realice estas operaciones y establezca el caso inicial.

Por ejemplo, el IC3 puede identificar a 100 víctimas y llegar a la conclusión de que la actividad delictiva parece tener su origen en un servidor radicado en Canadá, pero, en realidad, ese servidor no es más que una máquina comprometida. Los delincuentes la están utilizando como "punto de rebote" para ocultar su verdadera ubicación. Así pues, para los agentes del IC3 es muy importante saber más sobre el punto de rebote. Puede ser que un grupo radicado en Texas, África occidental o Rumania esté utilizando el servidor en Canadá para recoger información sobre posibles víctimas.

Alianzas con la industria

Dado que los analistas del IC3 han comprobado que, en algunos casos técnicos complicados, es mejor seguir el rastro inicial de la investigación, el Centro ha fundado para tal fin, en Pittsburgh, Pennsylvania, la Oficina de Iniciativa y Fusión de Recursos Cibernéticos (OIRFU). Los analistas de OIRFU eliminan las pistas falsas y trazan un perfil del caso antes de transmitirlo a un grupo especial o una agencia internacional de ejecución de la ley.

OIRFU es sostenida por las principales víctimas de los delincuentes cibernéticos, organizaciones y comerciantes en línea como Microsoft, eBay/PayPal y America Online, y asociaciones comerciales como Business Software Alliance, Direct Marketing Association, Merchant Risk Council, Financial Services Industry y otros. Los investigadores y analistas de estas organizaciones, muchos de los cuales ya están trabajando en asuntos relacionados con la delincuencia cibernética, han unido fuerzas con OIRFU para identificar las tendencias y tecnologías delictivas en Internet, establecer casos importantes y ayudar a los organismos encargados de la ejecución de la ley de todo el mundo a descubrir y combatir la delincuencia en Internet.



Fotomontaje: El International Crime Complaint Center y otras agencias de Estados Unidos trabajan con organizaciones internacionales como la Economic and Financial Crimes Commission (EFCC) de Nigeria y con funcionarios de ejecución de la ley de otros países para combatir el fraude en Internet. (Fotos de AP/Wide World Photos: Cabecera de la web facilitada amablemente por la EFCC).

En el OIRFU, agentes y analistas de la industria y las universidades trabajan juntos para averiguar dónde se origina el delito, quién se oculta detrás de él y cómo combatirlo. Cuando el OIRFU recibe información a través de un grupo industrial de una tendencia o problema concretos, elabora un plan para poner en el punto de mira a algunos de los principales delincuentes, efectuar arrestos y, no sólo procesarlos, sino aprender todo lo posible de su forma de actuar. Entonces, el IC3 informa al público de las tendencias y fraudes mediante un aviso que publica en su sitio de la web o divulga por otros medios.

Sobre la base de las denuncias presentadas por los consumidores y los datos proporcionados por la industria, los investigadores vigilan las tendencias y los problemas y elaboran planes de seis a 12 meses, con socios de la industria, contra determinadas actividades delictivas, entre las que se cuentan las siguientes:

- **Reenviar:** operación consistente en la contrata de conspiradores o cómplices inconscientes en Estados Unidos, encargados de recibir mercancía electrónica o de otra índole, adquirida con tarjetas de crédito robadas o fraudulentas, y embalarla de nuevo para su envío, generalmente al extranjero. Cuando el comerciante descubre que la tarjeta de crédito es fraudulenta, la mercancía ya está en otro país.
- **Spam delictivo:** envío de numerosos mensajes por correo electrónico para fines ilícitos no solicitados con intento de defraudar a instituciones financieras, cometer fraude con tarjetas de crédito, robo de identidad y otros delitos. También se puede utilizar para obtener acceso a ordenadores y servidores sin autorización y transmitir virus e instalar programas informáticos invasores en otros ordenadores.
- **"Phising":** Intento de robar contraseñas e información financiera bajo la falsa apariencia de un individuo o una empresa de confianza, en una comunicación electrónica, aparentemente oficial, como un correo electrónico o un sitio en la web.
- **Robo de identidad:** Utilización por un delincuente de la información personal de otra persona robada para cometer fraude u otros delitos. Unos pocos datos personales es todo lo que se necesita para robar una identidad.

Alcance internacional

El IC3 también trabaja con organizaciones internacionales como la Comisión para la Lucha contra los Delitos Económicos y Financieros (EFFCC) de Nigeria, donde una gran cantidad de delitos económicos y financieros como el blanqueo de dinero y el fraude relativo al pago de comisiones por adelantado han tenido graves consecuencias para el país.

El fraude 419, nombre con el que se le conoce por la Sección del Código Penal de Nigeria infringe, combina la amenaza del robo de identidad con la variante de una estratagema de pago de comisión por adelantado. Una víctima potencial recibe una carta por correo ordinario, electrónico o fax de alguien que se hace pasar por funcionario de Nigeria o de otro país, en la que se le

pide ayuda para colocar grandes sumas de dinero en cuentas bancarias en el extranjero a cambio de una participación en las ganancias. El plan consiste en convencer a una víctima de que envíe dinero al remitente a plazos, por diversos motivos.

En Nigeria, la amenaza de estos delitos condujo al establecimiento de la EFCC. En el curso del último año y medio, el IC3 ha confiscado grandes cantidades de mercancías y efectuado numerosos arrestos en África occidental, como resultado de ésta y otras alianzas.

El IC3 también trabaja en estrecha colaboración con la organización canadiense Denuncia de Delitos en Línea (RECOL). RECOL está administrado por el Centro Criminal y cuenta con el apoyo de la Policía Montada Real del Canadá y otros organismos. RECOL es una asociación de organismos de ejecución de la ley internacionales, federales y provinciales, y organismos reguladores y entidades comerciales privadas que tienen un interés legítimo en recibir denuncias de delitos económicos.

Un grupo cada vez mayor de organismos internacionales está empeñado en combatir la delincuencia cibernética. El IC3 trabaja con agentes de ejecución de la ley en muchos países, entre ellos Australia y el Reino Unido. Representantes del IC3 asisten a reuniones periódicas de la sección de delitos de alta tecnología del G8 (Alemania, Canadá, Estados Unidos, Francia, Italia, Japón, el Reino Unido y Rusia), parte de la cual se dedica a combatir la delincuencia cibernética y mejorar las investigaciones cibernéticas.

Los proyectos del IC3 y el OIRFU están en continua evolución. Mientras se están llevando a cabo, agentes y analistas del IC3 observan lo que está y lo que no está dando resultado y constantemente buscan expertos y fuentes de inteligencia para aprender más sobre la delincuencia cibernética y cómo combatirla con más eficacia. Ésta es la tarea constante del IC3.

Fuente:
http://usinfo.state.gov/journals/itgic/0306/ijgs/larkin.htm

Crimen organizado y crimen cibernético: sinergias, tendencias, y respuestas

Por Phil Williams

Muchos gobiernos, empresas comerciales y personas particulares en todas partes del mundo recién están empezando a aprender cómo aprovechar al máximo las últimas tecnologías informáticas. Pero las empresas del crimen organizado ya han descubierto que estas tecnologías ofrecen nuevas oportunidades de explotación y ganancias ilegales.

Las capacidades y oportunidades provistas por la Internet han transformado muchas actividades comerciales legítimas, al aumentar la rapidez, la facilidad y el alcance con que se pueden llevar a cabo las transacciones, reduciendo al mismo tiempo muchos de los costos. Los delincuentes han descubierto también que la Internet puede ofrecer nuevas oportunidades y multiplicar los beneficios de los negocios ilícitos. El lado sombrío de la Internet no solamente incluye fraude y robo, pornografía y redes de pedofilia, sino también narcotráfico y organizaciones criminales más inclinadas a la explotación que a la desorganización que procuran los piratas de la informática.

En el mundo virtual, igual que en el mundo real, las actividades criminales son iniciadas mayormente por individuos o grupos pequeños y se las puede entender mejor como "crímenes desorganizados". Pero hay pruebas crecientes de que existen grupos del crimen organizado que explotan las nuevas oportunidades ofrecidas por la Internet. El crimen organizado y el crimen cibernético nunca serán sinónimos. El crimen organizado seguirá actuando mayormente en el mundo real y no en el mundo cibernético, y el crimen

cibernético será perpetrado por individuos y no por organizaciones criminales. Sin embargo, el grado de coincidencia entre los dos fenómenos probablemente aumentará considerablemente durante los próximos años.

Crimen organizado y crimen cibernético

El crimen organizado trata principalmente de la búsqueda de ganancias y se lo puede entender, en términos Clausewitzianos[1] como una continuación de los negocios por medios delictivos. Por consiguiente, igual que las compañías de ladrillos y argamasa trasladan sus empresas al World Wide Web en procura de nuevas oportunidades de ganancias, las empresas delictivas están haciendo lo mismo. Las organizaciones criminales no son los únicos participantes en los mercados ilícitos, pero muchas veces son los más importantes, no sólo debido a la "competitividad" adicional que provee la amenaza de la violencia organizada. Además, las organizaciones criminales tienden a ser excepcionalmente hábiles en identificar y aprovechar oportunidades para nuevas empresas y actividades ilegales. En este contexto, la Internet y el crecimiento continuo del comercio electrónico ofrecen nuevas y enormes perspectivas de ganancias ilícitas.

En años recientes los grupos del crimen organizado y del narcotráfico se han refinado enormemente. Las organizaciones narcotraficantes colombianas, por ejemplo, emplean prácticas empresariales regulares de diversificación de mercados y productos, y explotan los nuevos mercados en Europa Occidental y la ex Unión Soviética. Las organizaciones delictivas y del narcotráfico emplean en forma creciente especialistas financieros para llevar a cabo sus transacciones de lavado de dinero. Esto agrega una capa extra de protección, al utilizar expertos jurídicos y financieros informados en transacciones financieras y en la existencia de refugios en jurisdicciones financieras extraterritoriales. Al mismo tiempo, el crimen organizado no necesita desarrollar su experiencia técnica en cuanto a la Internet. Puede contratar a aquellos de la comunidad de piratas informáticos que tienen esa experiencia, asegurándose mediante una combinación de recompensas y amenazas de que lleven a cabo en forma efectiva y eficiente las tareas que les son asignadas.

Los grupos del crimen organizado generalmente tienen bases en los estados débiles que les proveen un refugio desde el que pueden realizar sus operaciones transnacionales. En efecto, esto les da un grado adicional de protección contra las autoridades y les permite operar con un mínimo de riesgo. La inherente naturaleza transnacional de la Internet se ajusta perfectamente a este modelo de actividad y al esfuerzo de aumentar al máximo las ganancias con un grado de riesgo aceptable. En el mundo virtual no existen fronteras, una característica que lo hace muy atractivo para las actividades criminales. Pero cuando las autoridades tratan de controlar este mundo virtual, descubren que las fronteras y las jurisdicciones nacionales son grandes --lo que hace que una investigación a fondo sea, en el mejor de los casos, lenta y tediosa y en el peor de los casos imposible.

La Internet misma ofrece oportunidades para varios tipos de robos, ya sea de bancos que operan en línea o de propiedades intelectuales. Pero ofrece también medios nuevos para cometer crímenes antiguos como fraude, y ofrece nuevas vulnerabilidades en lo que respecta a comunicaciones y a información, lo que proporciona víctimas propicias para la extorsión, que siempre ha sido un delito clásico de la Mafia.

La anonimidad de la Internet hace que ésta sea también un conducto y un instrumento ideal para muchas actividades del crimen organizado. La noción del hampa connota tenebrosidad o falta de transparencia. El secreto generalmente es una parte clave de la estrategia del crimen organizado y la Internet ofrece oportunidades excelentes para mantenerlo. Se puede ocultar los actos detrás de un velo de anonimidad, el que puede abarcar desde el uso de los cafés cibernéticos omnipresentes hasta los complejos intentos de encubrir el encaminamiento en la Internet.

El crimen organizado ha escogido siempre industrias

particulares como objetivos de infiltración y para ejercer su influencia ilícita. En el pasado, figuraron entre éstas las industrias del transporte de basura y de la construcción en Nueva York, las industrias de la construcción y de la eliminación de desperdicios tóxicos en Italia, y las industrias de la banca y del aluminio en Rusia. Desde el punto de vista del crimen organizado, la Internet y el crecimiento del comercio electrónico presentan nuevos objetivos de infiltración y ejercicio de influencia -- perspectiva que sugiere que la tecnología y las firmas de servicios de la Internet deben cuidarse particularmente de sus socios y financiadores futuros.

En pocas palabras, la sinergia que existe entre el crimen organizado y la Internet no solamente es muy natural sino que también es propensa a florecer y desarrollarse aún más en el futuro. La Internet provee los conductos y también las víctimas para el crimen y permite que éstas sean explotadas para proveer ganancias considerables con muy poco riesgo. El crimen organizado no puede pedir más. Por lo tanto, es vital que se identifiquen algunas de las maneras en que el crimen organizado ya coincide con el crimen cibernético.

Tendencias principales del crimen organizado y crimen cibernético

Los grupos del crimen organizado utilizan la Internet para fines de fraude y robo. Tal vez el ejemplo más notable de esto - si bien uno que no tuvo éxito - ocurrió en octubre de 2000 y tuvo que ver con el Banco de Sicilia. Un grupo de aproximadamente veinte personas, algunas conectadas con familias de la Mafia, en combinación con un empleado del banco, crearon un clon digital del elemento en línea del banco. El grupo se propuso utilizar esto para desviar unos 400 millones de dólares que la Unión Europea había asignado para proyectos regionales en Sicilia. El dinero habría de ser lavado por intermedio de varias instituciones financieras, incluso el banco del Vaticano y bancos en Suiza y Portugal. El plan fue desbaratado cuando uno de los miembros del grupo informó a las autoridades. - Pero reveló claramente que el crimen organizado percibe que hay enormes oportunidades de ganancias como resultado del crecimiento de la banca y comercio electrónicos.

En efecto, la diversificación del crimen organizado en varias formas de crímenes en la Internet está estrechamente relacionada con una segunda tendencia discernible - el involucramiento del crimen organizado en lo que anteriormente se categorizaba como crímenes financieros. Las actividades de la Mafia norteamericana y las organizaciones criminales rusas en Wall Street pertenecen a esta categoría. Durante los últimos años de la década de 1990 hubo numerosos casos en que organizaciones criminales manipularon acciones de microfichas, empleando las técnicas clásicas de "recoger y descargar". Aunque una gran parte de esto se hacía mediante la coerción o el control de las firmas bursátiles, se utilizaba también la Internet para distribuir información que inflaba artificialmente el precio de las acciones.

Entre los involucrados había miembros de las familias criminales de Bonnano, Genovese y Colombo, así como inmigrantes rusos miembros del grupo criminal Bor. Al apartarse las organizaciones criminales de sus "actividades de fuerza" más tradicionales y concentrarse más en las oportunidades que les brindan los crímenes financieros, las actividades basadas en la Internet se extenderán más aún. Puesto que el fraude bursátil relacionado con la Internet resulta para los inversionistas en una pérdida de 10.000 millones de dólares anuales, el mismo ofrece un área particularmente lucrativa para el crimen organizado.

Esto no sugiere que el crimen organizado cambiará de carácter. Su disposición inherente a usar la fuerza y la intimidación se presta bien para el desarrollo de refinadas maquinaciones de extorsión cibernética con las que tratan de interrumpir los sistemas de información y comunicación y destruir datos. En efecto,

el crecimiento de la extorsión cibernética es una tercera tendencia significativa. Algunas veces se chapucean los planes de extorsión, pero se los puede llevar a cabo en forma anónima incurriendo solamente en pequeños riesgos, mientras siguen produciendo grandes ganancias. En efecto, ésta ya puede ser una forma de delito sobre el que no se informa suficientemente. Pero es también una forma de delito que podemos anticipar que se expandirá considerablemente al dedicarse el crimen organizado a explotar con entusiasmo las vulnerabilidades que acompañan la creciente dependencia de los sistemas concatenados.

Una cuarta tendencia es la utilización de lo que inicialmente fueron instrumentos de fastidio para la realización de actividades criminales más abiertas. Quizás el ejemplo más notable de esto ocurrió a fines del 2000, cuando se utilizó una variación del virus conocido como "love bug" en un intento de ganar acceso a contraseñas de cuentas del Union Bank de Suiza y por lo menos dos bancos en Estados unidos. Si bien este episodio recibió poca atención -y no se sabe bien quiénes fueron los perpetradores- hace más creíble la teoría de que el crimen organizado se está relacionando con piratas técnicamente especializados.

Una quinta tendencia cuya aparición podemos anticipar es lo que podría llamarse arbitraje jurisdiccional. El crimen cibernético -ciertamente si está vinculado con el crimen organizado- comenzará cada vez más en jurisdicciones que tienen pocas o ningunas leyes dirigidas contra él. Esta fue una de las lecciones del virus "love bug". Aunque el virus se propagó por todo el mundo y costó al sector comercial miles de millones de dólares, cuando agentes de la FBI lograron identificar al perpetrador, un estudiante en las Filipinas, descubrieron también que no había leyes para enjuiciarlo. Las Filipinas, subsecuentemente, adoptaron medidas para prohibir los crímenes cibernéticos, y otros países las siguieron. Pero todavía existen vacíos jurisdiccionales que permiten a delincuentes y piratas operar impunemente.

En efecto, es posible que algunas de las jurisdicciones procuren asumir una actitud tolerante con el fin de atraer negocios y crear santuarios informáticos (parecidos a los paraísos tributarios extraterritoriales y las jurisdicciones de confidencialidad bancaria) que hacen que sea difícil para las autoridades seguirle los rastros a la información, y ofrezcan proteger las transacciones comerciales cibernéticas mediante las cuales las empresas ilícitas pueden operar con un mínimo de interferencia.

Una sexta tendencia es que se utilice la Internet para el lavado de dinero. A medida que la Internet se convierte en el medio con que el comercio internacional lleva a cabo más y más negocios, aumentarán probablemente las oportunidades de lavar dinero mediante la facturación fraudulenta. Las subastas en línea ofrecen oportunidades similares para mover el dinero a través de compras aparentemente legítimas, pero pagando mucho más que lo que valen los bienes. El juego de azar en línea también hace posible mover dinero -especialmente hacia los centros financieros extraterritoriales en el Caribe. Además, al propagarse el dinero electrónico y la banca electrónica, también aumentan las oportunidades de ocultar el movimiento de los productos del crimen en un fondo creciente de transacciones ilegales.

Una séptima tendencia incluye la creciente concatenación entre los piratas cibernéticos o delincuentes de poca monta y el crimen organizado. En septiembre de 1999, por ejemplo, se condenó y encarceló a dos miembros de un grupo establecido en Estados Unidos conocido como "Phonemasters", por haber penetrado los sistemas informáticos de las compañías de telecomunicaciones MCI, Sprint, AT&T y Equifax. Uno de los convictos, Calvin Cantrell, había descargado miles de números de tarjetas de llamadas de Sprint. Los números fueron vendidos a un canadiense, vueltos a pasar por Estados Unidos, revendidos a otro individuo en Suiza y, por último, las tarjetas de llamadas terminaron en manos de grupos criminales en

Italia. Las concatenaciones entre los dos tipos de grupos probablemente aumentarán.

Además, el crimen organizado utiliza la Internet con fines de comunicación (usualmente codificada) y con otros propósitos cuando considera que su uso es útil y lucrativo. En efecto, el crimen organizado demuestra ser flexible y adaptable en su aprovechamiento de las oportunidades cibernéticas, igual que lo hace con otras oportunidades de actividades ilegales. Las implicaciones son de gran alcance y requieren del gobierno una respuesta de naturaleza estratégica, de muchos niveles, multilateral y transnacional.

Respuestas nacionales e internacionales a la sinergia del crimen organizado y el crimen cibernético

La respuesta a la creciente coincidencia entre el crimen organizado y el crimen cibernético exige una estrategia completa. Existen precedentes y modelos para esto que pueden ser particularmente útiles, que incluso toman en cuenta la necesidad de equilibrar los intereses policiales y de seguridad nacional con consideraciones tales como la confidencialidad personal. Un buen modelo para esto pueden ser los principios claves que han servido de guía a las respuestas de la comunidad internacional al crimen organizado y lavado de dinero transnacionales.

El Grupo de Trabajo de Acción Financiera (GTAF), organismo establecido por el G-7, ha intentado crear normas y pautas que los gobiernos e instituciones financieras pueden utilizar en la creación de leyes, reglamentos y mecanismos de aplicación a nivel nacional. Si bien se puede criticar al GTAF, éste inició en 2000 una campaña eficaz de "nombrar y avergonzar", la que identificó a 15 jurisdicciones "no cooperadoras" cuyos esfuerzos para combatir el lavado de dinero eran extremadamente insuficientes. En algunos casos, los resultados fueron notables y resultaron en programas más estrictos contra el lavado de dinero y en una mayor transparencia de las actividades financieras.

Aunque la campaña del GTAF fue la culminación de diez años de trabajo, ofrece, sin embargo, un planteamiento que la comunidad internacional puede emular con provecho al dedicarse a combatir el crimen cibernético. La Convención sobre el Crimen Cibernético aprobada por el Consejo de Europa y respaldada principalmente por Estados Unidos, señala el primer paso importante en esta dirección y se la puede considerar el comienzo del proceso de fijar normas y pautas que por último se esperará que los gobiernos nacionales satisfagan en sus gestiones legislativas, regulatorias y policiales.

El planteamiento de la Convención se basa en el reconocimiento fundamental de que se necesita armonizar las leyes nacionales. En años recientes, se ha logrado la cooperación internacional en materia de aplicación de la ley mediante una serie de tratados de extradición y ayuda jurídica mutua, que permite a los gobiernos intercambiar información y pruebas. Sin embargo, para que los los tratados de extradición y ayuda jurídica mutua entren en vigor, generalmente existe un requerimiento de criminalidad doble (es decir, el acto delictivo debe ser calificado como tal en ambas jurisdicciones). En otras palabras, la cooperación internacional se facilita enormemente con la convergencia de lo que es penalizado en las jurisdicciones nacionales.

Además, según lo señaló Ernesto Savona, director del Centro de Investigación de Crímenes Transnacionales en Trento, Italia, la imposición de leyes similares en varios países propaga los riesgos que las organizaciones delictivas deben confrontar y al mismo tiempo sirve para igualar los riesgos a través de las jurisdicciones. De hecho, cuanto más alcance tengan las leyes, tanto menor será el número de refugios desde los que los piratas controlados por el crimen organizado (o en efecto piratas individuales) puedan operar con

impunidad.

La armonización es necesaria tanto para las leyes substantivas como las procesales. Todos los países deben reevaluar y revisar sus reglamentos acerca de las pruebas, el registro y decomiso, la escucha electrónica oculta y otras actividades similares, que abarquen la información digital, los sistemas modernos de computación y comunicación y la naturaleza mundial de la Internet. Una mayor coordinación de las leyes procesales facilitaría, por lo tanto, la cooperación en las investigaciones que trasciendan jurisdicciones múltiples.

Además de tener las leyes apropiadas, es importante también que los gobiernos y las instituciones de aplicación de la ley desarrollen la capacidad para poner en vigor esas leyes. Esto requiere que se adquiera experiencia en el área del crimen cibernético y que también se establezca un intercambio eficaz de información entre las instituciones, tanto dentro de un país como a través de las fronteras nacionales. Asimismo, este intercambio deberá extenderse más allá de los organismos tradicionales de aplicación de la ley y deberá incluir a los organismos de seguridad nacional y de inteligencia.

Es esencial también que se formen unidades policiales especializadas para abordar cuestiones del crimen cibernético a nivel nacional. Estas unidades pueden servir también de base tanto para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley. La cooperación ad hoc y los grupos especiales multinacionales pueden resultar ser particularmente útiles- y ya hay casos en que la cooperación internacional ha sido muy efectiva. De hecho, la cooperación puede engendrar emulación y éxitos adicionales.

El otro elemento importante de una estrategia para combatir el crimen cibernético es la asociación entre los gobiernos y la industria, especialmente en el sector de la tecnología informática. En esto también hay precedentes. En años recientes, las principales compañías petroleras, si bien muy competitivas las unas con las otras, establecieron sistemas de intercambio de información y colaboraron estrechamente con las autoridades policiales para reducir al mínimo la infiltración de figuras del crimen organizado y de empresas delictivas. Este tipo de cooperación de los sectores gubernamentales y privados no siempre es fácil, pero no hay duda que un grado de confianza mutua puede significar mucho.

Para que se extienda la cooperación, las autoridades de aplicación de la ley deben ser muy cuidadosas y discretas en el sentido de no exponer las vulnerabilidades de la compañía, y al mismo tiempo las compañías mismas deben estar dispuestas a denunciar cualesquiera actividades criminales en contra de sus sistemas de información y comunicación.

Aun si se lograra un progreso considerable en todas estas áreas, el crimen organizado y el crimen cibernético seguirán floreciendo. Pero, si se toman medidas en estos sentidos, habrá por lo menos una posibilidad de que se pueda contener el crimen cibernético dentro de límites aceptables, de modo que no socave la confianza en el comercio electrónico, que no enriquezca a los grupos del crimen organizado de modo que puedan pervertir y amenazar aún más a los gobiernos, y que no sea el crimen organizado el que gane más con la Internet.

---

[1] Se refiere al filósofo alemán Karl von Clausewitz, reconocido por la máxima "La guerra es una continuación de la política por otros medios". al texto

El profesor Williams es catedrático del Colegio de Estudios en Asuntos Públicos e Internacionales de la Universidad de Pittsburgh. También es director de la publicación Transnational Organized Crime en http://www.pitt.edu/~rcss/toc.html. Se puede obtener información adicional sobre seguridad en la Internet en http://www.cert.org/

Fuente:
http://usinfo.state.gov/journals/itgic/0801/ijgs/gj-7.htm

Recursos en Internet

Instituto de Comité de Auditoría. Prevención de Fraudes
http://www.kpmg.com.mx/gobiernocorporativo/html/fraude.htm

Delincuencia informática e internet
http://www.utem.cl/cyt/derecho/delitos.html

La lucha contra la delincuencia en Internet
http://www.onu.org/Agenda/conferencias/delito/np07.htm

Internet y delito informático: nuevas formas de criminalidad?
http://www.alfa-redi.org/rdi-articulo.shtml?x=818

Propuestas legislativas buscan controlar el robo de identidad
http://www.oag.state.ny.us/press/2005/apr/apr18a_05_spanish.html

Robo de identidad
http://www.chicago.bbb.org/idtheft/IDTheftSpanish/identity.html

Comisión Federal de Comercio: su fuente nacional de recursos sobre robo de identidad
http://www.consumer.gov/idtheft/espanol.htm

Co**operación interjurisdiccional: un caso de delincuencia cibernética**
http://usinfo.state.gov/journals/itdhr/1003/ijds/green.htm

Tome control: defiéndase contra el robo de identidad
http://www.ftc.gov/bcp/conline/spanish/credit/s-idtheft.htm

Delitos y abusos en el comercio electrónico
http://www.jrc.es/pages/iptsreport/vol57/spanish/ICT2S576.htm

Delitos transnacionales relacionados con computadoras: los delitos del mañana a nuestras puertas
http://www.unodc.org/palermo/cybercrimeS.doc

Reporte los incidentes de seguridad
http://www.symantec.com/region/mx/smallbusiness/articles/LAM_report.html

Recomendaciones de la Tercera Reunión del Grupo de Expertos Gubernamentales en Materia de Delito Informático
http://www.oas.org/juridico/spanish/cybGE_IIIinf8.pdf

La lucha contra el delito en línea electrónica
http://usinfo.state.gov/journals/itgic/0306/ijgs/larkin.htm

Convenio sobre cibercriminalidad, Budapest, 23.XI. 2001
http://www.interpol.int/Public/TechnologyCrime/Conferences/6thIntConf/ConventionEs.pdf

Resolución 6ª Conferencia Internacional sobre Ciberdelincuencia
http://www.interpol.int/Public/TechnologyCrime/Conferences/6thIntConf/ResolutionEs.asp

Proyecto Norteamericano sobre Protección al Consumidor en Comercio Electrónico (NACPEC)
http://www.nacpec.org/es/index.html

Delito electrónico: Compilación
http://www.revistainterforum.com/espanol/pdfes/Compilacion-crimen-eletronico.pdf

Cibercrimen y legislación antiterrorismo
http://derechos.apc.org/handbook/ICT_22.shtml

Puntos mínimos regulatorios para la sociedad de la información en América Latina y el Caribe Bloque II
http://www.latinoamericann.org/documentos/pmr2.pdf

Hacia una correcta Hermenutica Penal - Delitos Informáticos vs. Delitos Electrónicos
http://www.alfa-redi.org/rdi-articulo.shtml?x=1480

Criminalidad informática: un fenomeno de fin de siglo
http://www.alfa-redi.org/rdi-articulo.shtml?x=267

Delitos Informáticos y Nuevas Formas de Resolución del Conflicto Penal
http://www.alfa-redi.org/rdi-articulo.shtml?x=1428

La necesidad de contemplar los Delitos Informáticos en el Código Penal del Estado de Michoacan
http://www.tribunalmmm.gob.mx/biblioteca/almadelia/indice.htm

- **Conceptos y antecedentes del Internet y de los Delitos Informáticos, su clasificación y características**
  http://www.tribunalmmm.gob.mx/biblioteca/almadelia/Cap3.htm
- **Legislación en diferentes países sobre los Delitos Informáticos**
  http://www.tribunalmmm.gob.mx/biblioteca/almadelia/Cap4.htm#4_1
- **Prácticas delictivas a través del Internet**
  http://www.tribunalmmm.gob.mx/biblioteca/almadelia/Cap5.htm

Bibliografía

1. **The cash connection: organized crime, financial institutions, and money laundering.** President's Commission on Organized Crime. Reprinted from the 1985 edition New York : Books for Business, 2001.

This interim report, which examines the problems of money laundering in the United States by organized crime, is the culmination of an effort by the members and staff of the Commission. The report sets forth substantial administrative and legislative recommendations.

2. **Networks and netwars: the future of terror, crime, and militancy.** Santa Monica, CA : RAND, 2001.

Netwar-like cyberwar-describes a new spectrum of conflict that is emerging in the wake of the information revolution. Netwar includes conflicts waged, on the one hand, by terrorists, criminals, gangs, and ethnic extremists; and by civil-society activists (such as cyber activists or WTO protestors) on the other. To confront this new type of conflict, it is crucial for governments, military, and law enforcement to begin networking themselves.

3. Biegel, Stuart. **Beyond our control?: confronting the limits of our legal system in the age of cyberspace.** Cambridge, Mass. : MIT Press, c2001.

Provides a framework for thinking about the law and cyberspace, examining the extent to which the Internet is currently under control and the extent to which it can or should be controlled.

4. Richards, James R. **Transnational criminal organizations, cybercrime and money laundering: a handbook for law enforcement officers, auditors, and financial investigators.** Boca Raton, FL : CRC Press, c1999.

This book examines the workings of organized criminals and criminal groups that transcend national boundaries. Discussions include methods used by criminal groups to internationally launder money, law enforcement efforts to counteract such schemes, and new methods and tactics to counteract transnational money laundering.

5. Mussington, David. **Exploring money laundering vulnerabilities through cyberspace technologies: a Caribbean based exercise. Santa Monica**, CA : Critical Technology Institute. RAND, 1998

This report outlines the first steps in an emerging international dialogue on the promise and potential problems of cyberspace as an economic environment. It summarizes research performed by RAND for the Financial Crimes Enforcement Network of the U.S. Department of the Treasury.

6. Molander, Roger C. **Cyberpayments and money laundering: problems and promise.** Santa Monica, CA : RAND, 1998.

The purpose of this report and RAND's research was to explore with the public and private sector the potential vulnerabilities of new payment technologies to abuse by money launderers and other financial criminals.

Estas y otras obras pueden ser consultadas en el
Centro de Recursos Informativos Amador Washington
ubicado en el Edificio Clayton, Clayton (antiguo Edificio 520).
Teléfono: 207-7100 / Fax: 207-7363