Fraude informático, una amplia mirada

Diferencias de conceptos e implicaciones entre fraude, crimen cibernético y otros.

Joshsua González

Introducción

En la actualidad, simplificamos nuestras expresiones sobre el ámbito informático, reduciéndolas a la preposición "ciber" (cibercrimen, ciberterrorismo, ciberguerra, cibercomercio, cibereducación), cayendo en una definición utópica. El Departamento de Defensa de los Estados Unidos define el ciberespacio como *el entorno teórico en el que se comunica la información digitalizada, a través de redes informáticas*. Por otro lado, la Estrategia Nacional Militar para operaciones ciberespaciales del mismo país, define el ciberespacio como *el dominio que se caracteriza por el uso de la electrónica y del espectro electromag-nético para almacenar, modificar e intercambiar datos, mediante sistemas de redes e infraestructuras físicas*. Tiempo después, El Departamento de Defensa (en publicación junto al organismo de Operaciones Conjuntas, el 17 de septiembre 2006, incorporaron un cambio el 22 de marzo de 2010), define el ciberespacio como *un ámbito global en el entorno de la información. Se trata de la red interdependiente de infraes-*

tructuras tecnológicas de la información, incluida Internet, redes de telecomunicaciones, sistemas informáticos y procesadores embebidos. Tales medios utilizados en el ciberespacio como lo son la electrónica y el espectro electromagnético para almacenar, se enfocan en acciones como modificar e intercambiar datos, por medio de los sistemas en red. Las operaciones en el ciberespacio emplean las capacidades de este medio, principalmente para lograr dichos objetivos y contemplan operaciones de redes informáticas y actividades para operar y defender a la Red de Información Global.

Una nueva manera de delinquir

A casi 10 años de uno de los incidentes de seguridad mayor nombrados en el año 2008, donde un hombre conocido como Michael Largent fue arrestado por un proceso fraudulento en la creación de aproximadamente 58.000 cuentas bancarias, las cuales usó para el recaudo de dinero en transacciones electrónicas. Básicamente, Largent realizó una burla al sistema de Google Checkout, Paypal y otros sitios de transacciones, donde a través de transacciones mínimas de centavos logró acumular cerca de USD$50.000. Más allá del caso, las transacciones electrónicas en sí fueron válidas, no se halló delito punible en el acto de llegar a depositar centavos de dólar, por lo que a Largent no se le inculpó por este acto. El fraude se declaró en el hecho de llegar a falsificar nombres, números sociales y asociarlos a las cuentas bancarias, delito conocido como fraude bancario.

Lo que el crimen cibernético ha hecho es tomarse una gran cantidad de delitos ya existentes, con un vector diferente. La delincuencia informática es conocida hoy en día como un crimen o delito que utiliza ordenadores, dispositivos móviles, redes y computadores entre otros. Sin embargo, hay tres hechos distintos de estos crímenes, donde los equipos informáticos tienden a ser un objetivo, un arma, o simplemente un facilitador del acto.

En el primer caso, los sistemas informáticos son el objetivo del delito y foco de actividades tales como robo, destrucción, alteración de la información, sistemas de información y *software*. En el segundo caso, los equipos informáticos pretenden ser el arma que implica el uso para lanzar ataques, entre los que se cuentan: el acoso cibernético (*ciberbullying*), pornografía infantil, correo no deseado, *spoofing* (en calidad de suplantación de varios vectores, como sitios *web*, correo electrónico), DoS (Denegación de Servicio). De igual manera, en sus diferentes acciones (*Distributed Denial of Service DoS, Economic Denial of Service EDoS*). En el tercer caso, los sistemas de información, computadoras y elementos informáticos son el facilitador y apoyo a la delincuencia tradicional, tales como el robo, el asesinato y terrorismo, entre otros.

Generalmente, la ciberdelincuencia es considerada como un crimen regular con una nueva modalidad de realización y un medio que, de una u otra manera, es vinculado al uso de Internet, pero difiere un poco. Pues bien, la diferencia es la escala y el alcance de la delincuencia, que utilizando herramientas de escaneo automático pueden ser lanzadas a través de millones de personas en cuestión de minutos. Se opta por dichos medios, debido a las

acciones de los delincuentes y ofrece mayor seguridad e integridad física para éstos, con un nivel de exposición menor, capacidad de existencia de testigos y algo mucho más llamativo, la clandestinidad y persecución jurídica. Por ello, es posible que en cuestión de horas, todo el mundo podría ser cubierto con el mismo virus, gusano o cualquier otra cosa. ¿Cómo evolucionó? Realmente, la ciberdelincuencia comenzó como un *hobby* de informáticos aburridos y jóvenes estudiantes, cuyo objetivo principal era demostrar su destreza y mostrar sus habilidades como *hackers* a la comunidad de sus compañeros. Fueron personas con conocimientos un poco más avanzados, tratando de superarse unos a otros. A pesar de que algunos de los ataques causarían un grave perjuicio económico, los autores rara vez obtenían alguna remuneración económica de los ataques. Y en la mayoría de los casos, las víctimas son al azar, sin objetivos específicos.

Sin embargo, desde la década de los años 2000, se ha venido produciendo un cambio gradual hacia las redes del crimen y criminales más organizados, más que los piratas informáticos individuales. La delincuencia informática se ha convertido en un gran negocio. Y como se puede ver a partir de una serie de delitos informáticos y las violaciones que han ocurrido recientemente, ellos se están enfocando en las empresas que tienen bolsillos profundos financieros, de los que pueden obtener dinero. Un ejemplo que afecta a muchos es la información financiera y su hurto, como los números de tarjeta de crédito/débito. Hay un enorme mercado donde se pueden comprar números de tarjetas de crédito robadas. Y cuando la de tarjeta de crédito no funciona o se ha cerrado, en realidad se puede obtener un reembolso de vuelta.

Figura 1: Extraído de sitio web a través de la Deep web. Disponible en: 7jv2q5zyz4ij6yuf.onion

Se trata de un negocio real con diferentes características de delito cibernético. Uno de los principales fines es recopilar información financiera, secretos comerciales, sobre la disidencia, y cómo involucrar a las grandes corporaciones en situaciones que les representen riesgos.

Y, para cometer un delito no hay que tener grandes conocimientos tecnológicos. De ahí que la extorsión se ubique en el segundo grupo, cambiando sus vectores e ataque en el marco de tecnologías de uso diario, convertidas en un método infalible para el acto. Los casos más conocidos perpetrados por bandas criminales y exempleados poco conformes, quienes logran traspasar los mecanismos y controles de seguridad para amenazar con destruir los datos o revelar información privada, en caso de que no se llegara a pagar dinero por su silencio o protección.

Y, el tercer grupo contempla el fraude en Internet con diferentes modalidades. Por lo general, consiste en facilitar información falsa a un individuo específico o para toda la comunidad. Por ejemplo, las cotizaciones bursátiles pueden ser manipuladas, mediante la fabricación de información positiva o negativa para difundirla entre los participantes y generar subidas y bajadas en los mercados que afectan las acciones. Otra parte de la delincuencia acude al robo de identidad, en el cual los piratas informáticos pueden asumir la identidad de la víctima y asumir su *personaje* en Internet para hacer transacciones en línea o cualquier otro tipo de acciones. El verdadero problema más allá del delito es realmente la víctima, borrar el nombre de ellas de las listas de morosos, para obtener su historial de crédito restaurado, es un problema terrible.

Aun así, en nuestro país existen delitos cibernéticos poco típicos, que se ven como una conducta no delictiva, debido a la falta de una legislación más estricta. Es el caso de la piratería y aquellas acciones que van en contra de la propiedad intelectual.

La ciberdelincuencia también puede clasificarse con base en la sofisticación del medio utilizado. Técnicas criminales implican la intrusión en los ordenadores y las redes, además de *phishing/spoofing*, robo de identidad, denegación de servicio, ataques de suplantación, la manipulación de los servicios de datos, o el fraude. Y las características de estos crímenes incluyen un evento singular o discreto, siempre desde la perspectiva de la víctima, facilitado por *software* malintencionado, como los registradores de pulsaciones (*keyloggers*), *bots*,

Figura 2: Ejemplo de CryptoLoker, Extraído de Malwarebytes. Disponible en: http://images.techhive.com/images/article/2014/01/cryptolocker-100222101-orig.png

spyware, *backddors*, o troyanos. Las características de la delincuencia social contemplan el uso de herramientas legítimas como foros de los medios sociales, aplicaciones de mensajería y sitios *web* de citas. Y las actividades tales como el acoso, la depredación de los niños, la extorsión, el chantaje, el espionaje corporativo complejo y el ciberterrorismo son tipificados como delito.

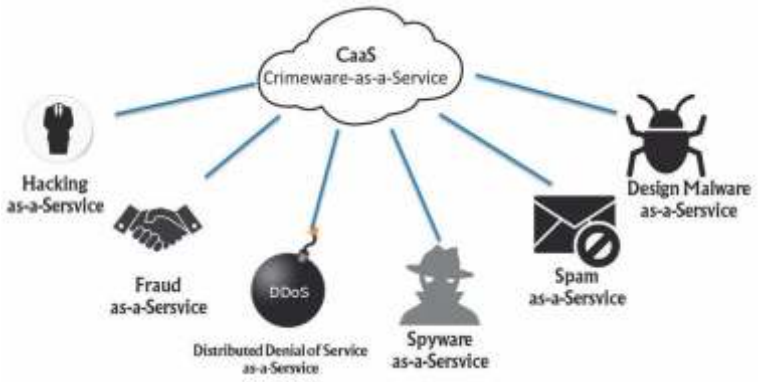
Crimeware, lo que es viejo es nuevo

En aspectos informáticos tenemos que cada tipo de *software*, según su propósito final, tiene un nombre característico. El *crimeware* debe ser diferenciado del *spyware*, *adware* y *malware*. El *crimeware* ha llegado a ser diseñado mediante técnicas de ingeniería social y de fraude, tanto *online* como *offline*, con el único propósito de robo de identidades para acceder a cuentas de compañías que tienden a pertenecer al sector financiero, compañías de comercio por internet y empresas de transacciones electrónicas. Se considera parte de fraude o crimen, debido a que estos programas están diseñados para robar o suplantar la identidad de una persona o usuario.

Hoy se utiliza tecnologías de punta, como lo son los servicios en la nube; de ahí que el *crimeware* sea identificado como *CaaS (Crimeware as a Service)*, donde las personas pueden llegar a escoger el tipo de servicio requerido. La característica más importante de dicho modelo de "negocio" es la clandestinidad que Internet llega a ofrecer, donde los esfuerzos en la parte legal llegarán a ser pieza clave para la persecución de los responsables.

Ciberterrorismo, nuevo campo de batalla

No sólo los fraudes, engaños, acosos, robos y accesos no autorizados se pueden considerar un crimen cibernético. Más allá, existe una amenaza estratégica, el ciberterrorismo. Según Denning, éste puede llegar a entenderse en la convergencia entre lo que es el terrorismo común, pero en un ámbito ciberespacial. Hecho que se basa en fallas, vulnerabilidades y riesgos tecnológicos para lograr intimidar o presionar a un Estado y su sociedad civil. La directiva presidencial Norteamericana No.13010 de 1998, define ocho sectores críticos con servicios vitales para el funcionamiento de la nación, cuya incapacidad de operación o destrucción tendría un



impacto directo en la defensa o en la seguridad económica:

1. energía eléctrica,
2. producción, almacenamiento y suministro de gas y petróleo,
3. telecomunicaciones,
4. bancos y finanzas,
5. suministro de agua,
6. transporte,
7. servicios de emergencia
8. operaciones gubernamentales (mínimas requeridas para atender al público)

El ciberterrorismo puede afectar infraestructuras críticas de un país: sistemas eléctricos, producción, almacenamiento y suministro de combustibles, telecomunicaciones, servicios financieros, sistema de suministro de agua, transporte, en todos sus ámbitos (aéreo, fluvial y terrestre).

Aspectos legales, no todo es tecnología

Es posible llegar a determinar que el ciberespacio se considera una nación globalizada extendida en un ámbito incorpóreo. La expresión comercio electrónico puede tomarse de manera genérica en su significado, mientras que el error que podemos llegar a cometer con el prefijo “ciber”, integra todo aquello intangible en ese meta-espacio.

En Colombia, el uso de un entorno digital y su desarrollo como nación en un ambiente ciberespacial presenta incertidumbres y exposición a riesgos en seguridad. Nuestro país ha hecho esfuerzos enormes en temas legales y procedimentales como lo son la ley de delitos informáticos 1273 del 2009, ley 1581 del 2012 protección de datos personales, ley 1623 de 2013 de inteligencia y criterios de seguridad y el documento CONPES 3854 sobre política nacional de seguridad digital, entre otros.

Sin embargo es posible que las normas nacionales sean inocuas, por ejemplo, para atacar la pornografía infantil o para proteger la confidencialidad de los datos personales. Este espacio global no sólo corresponde a la economía, sino también a otros aspectos sociales como la cultura, la religión, la raza y la política.

Actualidad y hacia dónde vamos

Considerando el ciberespacio como un nuevo sitio, un lugar donde prácticamente desaparece el paradigma de que lo real debe ser físico y tangible, persiste la sensación de cosas imaginativas debido a su particularidad de ser incorpóreo, un lugar diferente al mundo que conocemos. Por ese cambio de ambiente, también se percibe un cambio a nivel de competencias y un ordenamiento distinto. Tales razones llevan a considerar la

necesidad de una Constitución que le de vida a un nuevo Estado dentro de un marco normativo con reglas de incuestionable cumplimiento.

Es necesario tener avances en el proceso antes de lograr un nuevo estado global, y explorar formas más reducidas que agrupen diferentes naciones, hacia una sociedad global. El enfoque de la política de ciberseguridad y ciberdefensa, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de defensa y lucha contra el cibercrimen. Los esfuerzos del país han posicionado a Colombia entre los líderes regionales, pero es necesario estimular la gestión del riesgo en el ciberespacio junto con el desarrollo y evolución del marco jurídico.

Referencias

[1] Irvine, Cynthia (2014) *Security Education and Critical Infrastructures*

[2] Ventre, Daniel (2015) *Chinese Cybersecurity and Defense*

[3] Goodman, Marc (2016) *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*

[4] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL (2016) Política Nacional De Seguridad Digital. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[5] Denning, D (2000) *Cyberterrorism*. Disponible en: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[6] Suñé, Emilio (2012) *Declaración de Derechos del Ciberespacio* Disponible en: http://portal.uexternado.edu.co/pdf/7_convencionesDerechoInformatico/documentacion/conferencias/Los_Derechos_Humanos_en_el_Ciberespacio.pdf

[7] Gragido, Will & Pirc, John (2011) *Cybercrime and Espionage*

[8] Andress, Jason & Winterfeld Steve (2011) *Cyber Warfare*

Joshsua J. González Díaz, MSc. *Ingeniero de Sistemas de la Pontificia Universidad Javeriana, especialista en seguridad de la información de la Universidad de los Andes; especialista en Derecho Informático de la Universidad Externado de Colombia y Magíster en Seguridad de la Información de la Universidad de los Andes. Actualmente, se desempeña como profesor instructor de la maestría en Seguridad de la Información de la Universidad de Los Andes y CEO de la empresa de consultoría Stark Industries SAS.*