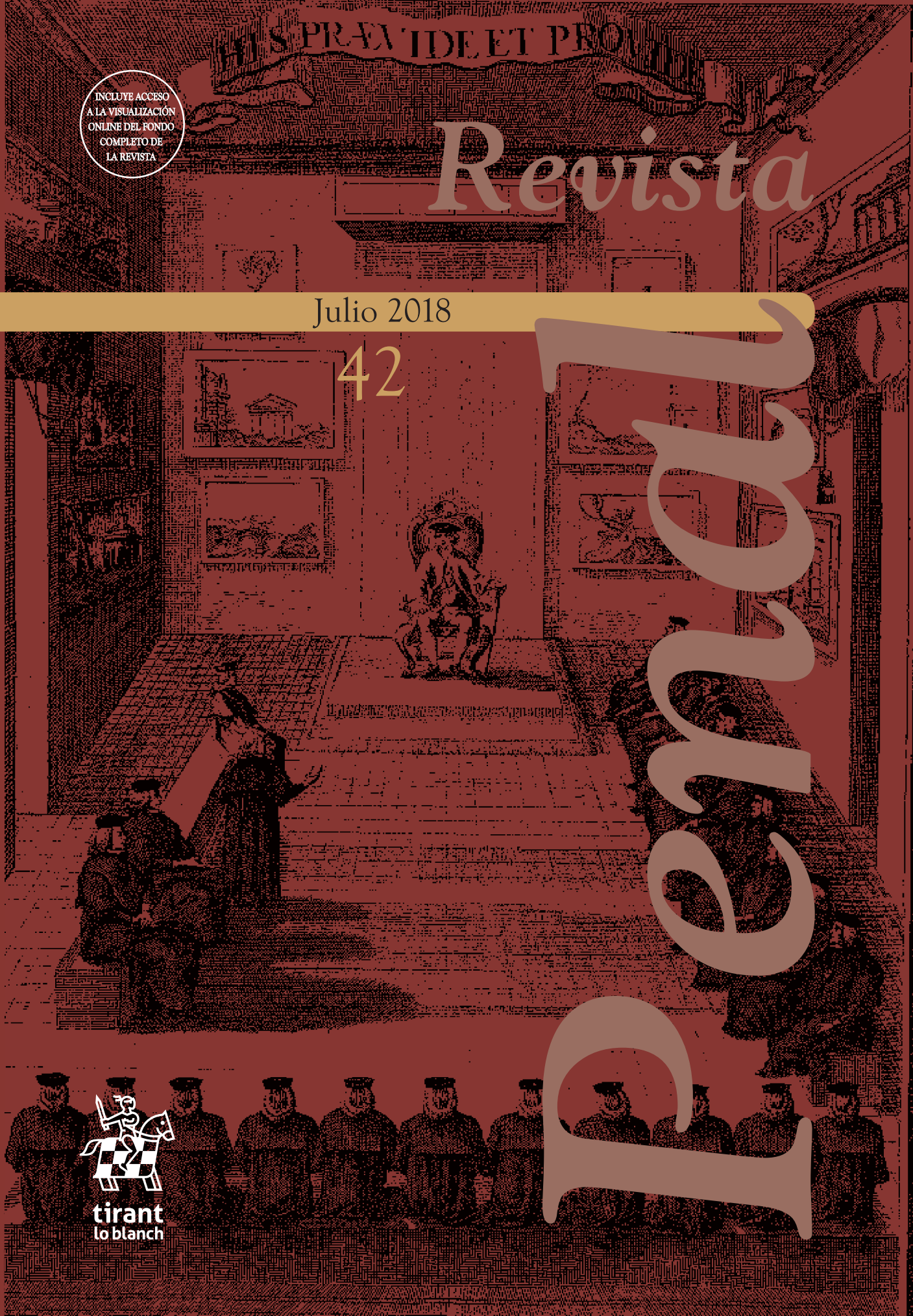
42

INCLUYE ACCESO A LA VISUALIZACIÓN ONLINE DEL FONDO COMPLETO DE LA REVISTA

Revista Penal

Julio 2018

42



tirant lo blanch

Revista Penal

Julio 2018

tirant lo blanch

Revista Penal

Número 42

Sumario

* *Los primeros 25 números de la Revista Penal están recogidos en el repositorio institucional científico de la Universidad de Huelva Arias Montano:* http://rabida.uhu.es/dspace/handle/10272/11778

tirant lo blanch

Publicación semestral editada en colaboración con las Universidades de Huelva, Salamanca, Castilla-La Mancha, Pablo Olavide de Sevilla y la Cátedra de Derechos Humanos Manuel de Lardizábal.

EDITA: TIRANT LO BLANCH
C/ Artes Gráficas, 14 - 46010 - Valencia
TELFS.: 96/361 00 48 - 50
FAX: 96/369 41 51
Email:tlb@tirant.com
http://www.tirant.com
Librería virtual: http://www.tirant.es
DEPÓSITO LEGAL: B-28940-1997
ISSN.: 1138-9168
IMPRIME: Guada Impresores, S.L.
MAQUETA: Tink Factoría de Color

El caso Wannacry. Ataque en la red

Alberto Enrique Nava Garcés

Revista Penal, n.º 42. - Julio 2018

Ficha Técnica

Autor: Alberto Enrique Nava Garcés
Código ORCID: orcid.org/0000-0002-1025-0850
Title: The Wannacry case. Attack on the network.
Adscripción institucional: Doctor en Derecho. Miembro del Sistema Nacional de Investigadores (Conacyt, México). Profesor por oposición de Derecho Penal en la Facultad de Derecho de la UNAM. Investigador Titular del Instituto Nacional de Ciencias Penales. Coautor del proyecto de Código Penal Nacional (México).

Resumen: en 2017, el número de ataques en la red se incrementó por diversos factores y por los múltiples motivos que nacen desde una oficina gubernamental hasta llegar a los ataques que se realizan con el mero fin de obtener una ganancia en el campo de la competitividad comercial. Pero ¿y si estos ataques incidieran en una campaña o en la jornada electoral? ¿qué riesgos generan esta clase de ataques a un estado democrático de derecho?

Palabras clave: ciberseguridad, Ataques DDos, Wannacry, Delitos informáticos, Internet.

Abstract: with the digital era, new challenges such as attacks on the net arrive. The law is constantly a step behind the new technologies and yet must solve big problems like this. How serious can an attack be on the net? What would happen if an attack was aimed at election day?

Key words: cybersecurity, DDos Attacks, Wannacry, Cybercrime, Internet.

Rec: 3-05-2018 **Fav:** 18-06-2018

148

I. INTRODUCCIÓN

En 2017, el número de ataques en la red se incrementó por diversos factores y por los múltiples motivos que nacen desde una oficina gubernamental hasta llegar a los ataques que se realizan con el mero fin de obtener una ventaja en el campo de la competitividad comercial.

Los ataques persiguen un fin esencialmente económico, sin embargo, la sustracción o el impedimento de acceso a los archivos no solo pueden ser precursores de la extorsión. Si no se prevén y no se legislan adecuadamente, se abre la posibilidad a que esta clase de conductas se propaguen a otros ámbitos como el electoral, con lo que además de producir incertidumbre sobre el resultado auténtico, pueden constituirse en una herramienta en las llamadas campañas sucias que empañen el proceso electoral o, en dado caso, produzcan su anulación, con las consecuencias económicas, políticas y sociales que ello implicaría[1].

1 Hace algunos años, David. E. Sanger, escribió para el New York Times: "Inicia era de la ciberguerra' Buscan disuadir ciberataques. En un programa secreto llamado 'Juegos Olímpicos', que data de los últimos años de la Administración de George W. Bush, Estados Unidos ha montado repetidos ataques con las armas cibernéticas más sofisticadas jamás desarrolladas. Ellas invadieron los controladores computacionales que operan las centrifugadoras nucleares de Irán, lo que las puso desbocadamente fuera de control.

Estados Unidos y su socio en los ataques, Israel, utilizaron estas armas como una alternativa a un ataque con bombas desde el aire. Sin embargo, Estados Unidos se niega a hablar sobre su nuevo arsenal cibernético, y nunca ha habido un verdadero debate sobre cuándo y cómo utilizar las armas cibernéticas.

El Presidente Obama planteó muchas de las problemáticas en el hermético santuario de la Sala de Situaciones, dicen varios participantes en la conversación, al presionar a los asistentes para que se aseguraran que los ataques estaban enfocados con precisión de manera que no trastocaran hospitales o centrales eléctricas iraníes y que estuvieran dirigidos únicamente contra la infraestructura nuclear del país. 'Él estaba sumamente enfocado en evitar el daño colateral', dijo un funcionario, al comparar los argumentos sobre usar la guerra cibernética con los debates respecto a cuándo utiliza aviones no tripulados Predator.

¿Acaso EU quiere legitimizar el uso de armas cibernéticas como una herramienta o encubierta? ¿O es algo que queremos mantener en reserva para casos extremos? ¿Acaso llegaremos al punto en que se querrán tratados para prohibir su uso?

Las armas cibernéticas, por supuesto, no tienen ni la precisión de un avión no tripulado ni el poder inmediato, horrendo y destructor de una bomba nuclear. La mayoría de las veces, la guerra cibernética parece fría y poco sanguinaria: computadoras que atacan a computadoras. A menudo así es.

Se cree que los chinos atacan los sistemas computacionales de estados Unidos a diario, pero principalmente para sustraer secretos corporativos y del Pentágono. EU a menudo hace lo mismo: los iraníes reportaron, a finales de mayo, que habían sido golpeados por otro ataque cibernético llamado 'Flame', que parecía recoger datos de laptops selectas, presuntamente de líderes y científicos iraníes.

Sin embargo, la vanguardia de la guerra cibernética está en la invasión de sistemas computacionales para manipular la maquinaria que mantiene en funcionamiento al país -precisamente lo que les hizo Estados Unidos a esas centrifugadoras iraníes. 'Alguien ha cruzado el Rubicón', comentó el General Michael V. Hayden, ex director de la CIA, al describir el éxito de los ataques cibernéticos contra Irán. Hayden tuvo cuidad de no decir qué papel jugó Estados Unidos, pero agregó: 'Ahora tenemos a una legión en el otro lado del río. No quiero fingir que es el mismo efecto, pero en un sentido, por lo menos, es agosto de 1945', el mes en que el mundo vio por primera vez las capacidades de una nueva arma, arrojada sobre Hiroshima y Nagasaki.

En marzo, la Casa Blanca invitó a todos los miembros del Senado a una simulación clasificada, realizada en el Capitolio, que demostró lo que podría ocurrir si un hacker dedicado -o un Estado enemigo- decidía apagar las luces en la Ciudad de NY. En la simulación un trabajador de la compañía eléctrica hacía click en lo que creía era un correo electrónico de un amigo; ese ataque 'Spear phishing' inició una cascada de desastres en el que el invasor cibernético se abrió paso hasta los sistemas computacionales que operan la red eléctrica de Nueva York. La ciudad quedó sumida en la oscuridad; nadie podía ubicar el problema.

La Administración hizo la demostración para presionar al Congreso a aprobar un proyecto de ley que permitiría un grado de control federal sobre la protección de las redes computacionales que operan la infraestructura más vulnerable de Estados Unidos. Nunca se habló de la verdadera razón de la simulación: la ofensiva cibernética ha rebasado la búsqueda de un elemento disuasivo, algo más o menos equivalente al concepto de la época de la guerra fría de la destrucción mutuamente asegurada. Había algo simple en ese concepto: Si tú eliminas Nueva York, yo elimino Moscú.

Sin embargo, no hay nada tan sencillo respecto a los ataques cibernéticos. Por lo general, es poco claro de dónde vienen. Es hace que la disuasión sea extraordinariamente difícil. Además, una buena disuasión 'tiene que ser creíble', señaló Joseph S. Nye, estratega de la Universidad de Harvard que ha escrito el análisis más profundo hasta ahora de qué lecciones de la era atómica se aplican a la guerra cibernética.

La disuasión también podría depender de cómo decida Estados Unidos utilizar sus armas cibernéticas en el futuro. ¿Acaso será más como el avión no tripulado Predator, una herramienta que el Presidente ha acogido?

Eso enviaría una clara advertencia de que Estados Unidos está listo y dispuesto a actuar. Sin embargo, como advirtió el Presidente Obama a sus propios asistentes durante los debates secretos sobre Juegos Olímpicos, también invita a ataques de represalia, con armas cibernéticas que ya proliferan

De hecho, un país hace poco anunció que estaba inmerso en la creación de nuevos 'Policías cibernéticos' de élite como parte de su ejército. El anuncio vino de Teherán." (*Reforma,* Sábado, junio 9, 2012. secc. The New York Times. pp. 1-2).

Gustavo Eduardo Aboso pone en contexto la gravedad de los ataques en la red:

En los Estados Unidos, después de los atentados terroristas del 11 de septiembre de 2001, el gobierno de ese país dictó la *USA Patriot Act* con el firme propósito de disponer de herramientas legales para la lucha contra el terrorismo. En especial, se incluyó de manera explícita por primera vez a la agresión ciberterrorista en la amplia lista de hipótesis delictivas. La Sección 814 de esa ley, titulada 'Disuasión y prevención del ciberterrorismo' (*'Deterrence and Prevention of Cyberterrorism'*), amplió la tutela penal a las computadoras situadas en el extranjero usadas por instituciones públicas, para el comercio exterior o las comunicaciones. También se incluyó en la lista de infracciones a los daños informáticos provocados en sistemas utilizados por los organismos de defensa, seguridad y administración de justicia.

Vinculado directamente con la prevención de esta clase de ataques cibernéticos, en Estados Unidos se sancionó en 2008 el robo de identidad (*Identity Theft Enforcement and Restitution Act*. Esta nueva ley amplió aún más el horizonte normativo de la *Computer Fraud and Abuse Act* de 1986 al eliminar cualquier tipo de restricción en materia de naturaleza o calidad de los sistemas o datos informáticos afectados.

El art. 183, en su párrafo segundo, de nuestro Código Penal reprime el delito doloso de daño informático.

En materia de terrorismo, la República Argentina establece en el art. 41 quinquies del Código Penal una causal de agravación de pena en función de hechos terroristas, en cuyo caso el marco punitivo previsto por el citado art. 183 debería aumentarse al doble en su mínimo y máximo.

También puede presentarse la posibilidad de que los *hackers* terroristas no se hayan limitado a la destrucción o alteración de un dato, programa o sistema informático, sino que su conducta haya estado orientada a defraudar económicamente al propio Estado o terceros. En este caso, el art. 173, inc. 16, del Código Penal argentino regula la estafa informática, que consiste en manipular un sistema informático, por ejemplo, de una institución bancaria o financiera, y producir una disposición automatizada de dinero electrónico de una cuenta corriente a otra. En este caso, como en el anterior, deberá sumarse el agravante especial previsto por el citado art. 41 quinquies, cuando ese hecho delictivo estuviese relacionado con un hecho terrorista. Si el perjudicado es la Administración pública, entonces deberá aplicarse a la citada figura de estafa informática el agravante previsto por el art. 174, inc. 5°.

Un intento de cooperación internacional en materia de cibercriminalidad ha sido el Convenio de Budapest de 2001, instrumento internacional que se afanó por armonizar las legislaciones penales a nivel mundial con el objetivo de crear un frente común en la lucha contra este fenómeno delictivo. En particular, el Capítulo II de este Convenio, y los arts. 4, 5 y 6, se ocupan de regular los ataques dirigidos contra los datos y sistemas informáticos, sumado a la punición anticipada de la producción, venta, importación y difusión de dispositivos idóneos para cometer delitos informáticos. De manera particular se pretende castigar la tenencia de dispositivos o programas informáticos con la intención de cometer estos delitos. Nuestro país carece de una norma penal que castigue de manera anticipada la mera tenencia de estos dispositivos o programas para la perpetración de delitos informáticos, pero otros países, como la República Federal de Alemania y España, ya regulan esta forma de represión anticipada de una conducta previa a la lesión de un bien jurídico determinado (§ 202c StGB y 248 del Código Penal español)[2].

Esta infracción penal recurre a la técnica de los delitos de peligro abstracto de la que se abastece generalmente el Derecho Penal de la seguridad. De esta forma, la represión de la tenencia de aparatos, dispositivos o programas idóneos para la comisión de delitos futuros como el acceso indebido a datos o sistemas informáticos o a la provocación de daños en esos sistemas resulta legitimada desde el punto de vista de un Derecho Penal orientado a la prevención, circunstancia que justificaría anticipar de manera desproporcionada las barreras de punición para abarcar conductas difusas. El elemento subjetivo resulta particularmente significativo para cifrar la necesidad de punición de estas conductas preparatorias. La tenencia de un programa dañino o virus informático habilitaría la intervención de las agencias gubernamentales para indagar sobre el propósito ulterior del autor. De esta manera se extiende el campo de acción de las fuerzas de prevención para intervenir en la vida personal de los ciudadanos. La mera sospecha de la tenencia de un programa de estas características o de un dispositivo o artefacto útil para la eventual comisión de un delito informático justificaría desde esta perspectiva la vigilancia electrónica de los sospechosos. Tarea hercúlea será la de probar de manera concluyente que el tenedor de ese programa o aparato había proyectado utilizarlo contra terceros[3/4].

Los ataques en la red son y deben ser esencialmente combatidos con la misma tecnología que son creados. El derecho siempre estará un paso atrás ante el advenimiento de estas conductas que en nuestros días se han convertido en una cuestión cotidiana, sin embargo, debe contener un marco general que permita su prevención y su castigo.

2 FISCHER, *StGB-K*, § 202c, marg. 1 y ss.

3 Ibídem; SCHUH, Computerstrafrecht im Rechtsvergleich, pp. 246 y ss.

4 Gustavo Eduardo Aboso, *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación.* Ed. B de f. Buenos Aires, 2017, pp. 420 - 422.

II. CASO: *WANNACRY*

Para tener una idea de la dimensión que puede tener un ataque en la red, partimos de un ejemplo que tuvo repercusión a nivel mundial. Entre los ataques más destacados que ocurrieron en 2017 (uno entre los cientos que pasaron y que llamaron la atención mundial) está el del programa denominado *"wannacry"* ("quiero llorar" en alusión a la reacción de los usuarios al perder su información), que es del tipo ransomware, cuya acepción deriva de conjuntar rescate con software y se trata de un programa (*malware*) que restringe el acceso a los archivos dañados. Cifra e inutiliza archivos y se propaga con muchísima facilidad, de moto tal que permite al sujeto activo coaccionar al usuario para devolverle el acceso a los archivos a cambio de un rescate, como lo establecimos líneas arriba[5].

Wannacry se convirtió en un ataque mundial el viernes 12 de mayo de 2017 que dejó inutilizado el software de un hospital en Inglaterra y más tarde, ya dispersado, causó daños en distintas instalaciones, algunas muy sensibles en distintas latitudes. A guisa de ejemplo, afectó más de setenta y cinco mil computadoras en el mundo, así como: La red de semáforos y el sistema de transporte subterráneo de Rusia; centros del sistema de salud del Reino Unido; empresas tales como: Telefónica, Gas Natural e Iberdrola en España y esta llamada infección se expandió por Estados Unidos, China, Italia y Taiwán, afectando en particular los sistemas operativos más vulnerables como son Windows Vista, Windows 7, Windows Server 2012, Windows 10 y Windows Server 2016.

Paradójicamente, se detuvo la expansión por un programador del Reino Unido que, días más tarde fue sometido a un proceso judicial relacionado con este tema[6].

---

5 Los ataques ciberfísicos han sido durante mucho tiempo una preocupación y llegaron a los titulares por primera vez el 23 de diciembre de 2015, cuando ciberataques pusieron la mitad de las casas en la región ucraniana de Ivano-Frankivsk en la oscuridad durante varias horas.

Pero tales ataques se están volviendo cada vez más comunes y el MIT predice que es probable que en el año 2018 aumenten los ataques cibernéticos contra redes eléctricas, sistemas de transporte y otros tipos de infraestructura crítica nacional.

Se espera que los ataques ciberfísicos estén diseñados para causar una interrupción inmediata o para amenazar con cerrar sistemas vitales para extorsionar a los operadores. MIT también predice que en 2018 los investigadores y atacantes descubrirán vulnerabilidades cibernéticas en aviones, trenes, barcos más antiguos y otros modos de transporte.

Otra tendencia que se espera que continúe y se amplíe en 2018 es el secuestro de poder de cómputo para minar criptomonedas al resolver problemas matemáticos complejos. Según la firma de seguridad Malwarebytes, bloqueó 11 millones de conexiones a sitios de minería de criptomonedas en un solo día en 2017.

MIT advierte que los atacantes cibernéticos que secuestran computadoras para la minería de criptomonedas podrían tener un efecto devastador si se dirigen a recursos informáticos en hospitales, aeropuertos y otras ubicaciones similares.

Finalmente, otra amenaza que se espera que continúe y se amplíe en 2018 son los ciberataques destinados a influir en las elecciones democráticas. Es ampliamente aceptado que atacantes de lengua rusa atacaron los sistemas de votación en 21 estados de los Estados Unidos antes de las elecciones presidenciales de 2016.

A pesar de los esfuerzos para abordar las vulnerabilidades antes de las elecciones de mitad de período en noviembre de 2018, MIT advierte que los atacantes decididos todavía tienen muchos objetivos potenciales, incluidos los registros electorales electrónicos, las máquinas de votación y el software utilizado para recopilar y auditar los resultados.

En junio de 2017, surgió que la votación en línea se retenía en el Reino Unido por temor a que los ciberdelincuentes pudieran influir en los resultados, con un 40% de los votantes del Reino Unido preocupados por el tema, según una encuesta justo antes de las elecciones del Reino Unido.

"Las afirmaciones de que los piratas informáticos rusos tuvieron cierta influencia en las elecciones presidenciales estadounidenses de 2016 han desatado una ola de escepticismo sobre la seguridad del voto electrónico en el Reino Unido", dijo Pete Turner, experto en seguridad del consumidor de Avast, que llevó a cabo la encuesta.

A la luz del plazo de cumplimiento del Reglamento General de Protección de Datos de la Unión Europea (GDPR), el 25 de mayo de 2018, es probable que las infracciones de grandes datos sean la máxima prioridad para cualquier organización que maneje los datos personales de ciudadanos de la UE, con multas de hasta a 20 millones de euros o el 4% de los ingresos globales, el que sea mayor.

Los corredores de datos que tienen información sobre cosas tales como los hábitos de navegación web personal de la gente probablemente estén entre los objetivos más populares para el compromiso, advierte el MIT. Consultado en http://searchdatacenter.techtarget.com/es/noticias/450432536/El-ransomware-le-pegara-a-la-nube-en-2018-predice-MIT?utm_medium=EM&asrc=EM_EDA_87646322&utm_campaign=20180105_Ocho%20ejecutivos%20de%20tecnolog%C3%ADa%20hablan%20sobre%20las%20tendencias%20de%20TI%20empresarial&utm_source=EDA el 14 de enero de 2018, 15:10 hs.)

6 En el periódico español El País se documentó el ataque: **El ciberataque: pulsar un botón y desenchufar el mundo.** Reconstrucción del ataque que paralizó los sistemas informáticos de más de 170 países. El próximo podría causar el caos a escala global.

Trabajadores de la Agencia de Seguridad e Internet de Corea del Sur analizan el alcance del ciberataque de WannaCry, el lunes.

El caso Wannacry. Ataque en la red

Ese viernes, Luis llegó muy temprano a la oficina. Dejaría unas cuantas tareas rutinarias finiquitadas y en unas horas estaría en Barajas tomando un vuelo a Mallorca. Su novia había comprado con mucha antelación los billetes y había reservado habitación en un hotel de cuatro estrellas. Todo estaba preparado, sería un fin de semana romántico con escapadas a calas ocultas y paseos en bicicleta. Sobre las diez, cuando apenas le faltaban unas horas para que se marchara y dejara atrás el calor de Madrid, algo empezó a salirse de control. Lo comprendió de inmediato. Las próximas 72 horas no iba a pasarlas frente al mar, como imaginaba, sino delante de un ordenador, encerrado entre cuatro paredes. El jefe de informáticos del servicio secreto español debe enfrentar una crisis mundial.

A esas horas, un virus de tipo ransomware (cibersecuestro) había infectado a 300.000 computadoras alrededor del mundo. La pantalla del usuario se fundía a negro y a los pocos segundos aparecía un mensaje en el que se le anunciaban que sus documentos habían sido encriptados (cifrados). En una breve explicación, disponible en 30 idiomas, se detallaba que si quería recuperarlos tenía que hacer un pago de 300 dólares a un número de cuenta en bitcoins, una moneda virtual difícil de rastrear. En la parte izquierda de la pantalla aparecían dos cronómetros, uno con el tiempo que tenía para realizar el pago y otro con el momento exacto en el que sus archivos serían destruidos. Más abajo, un teléfono de contacto. A menudo los hackers utilizan centros de atención telefónica para solventar cualquier duda del afectado e incluso para negociar una rebaja del precio, como los cárteles mexicanos hacen con los familiares de sus secuestrados.

El virus, bautizado WannaCry por sus creadores, se expandió el viernes 12 de mayo con una velocidad y una profusión pocas veces vista. Los atacantes, según los expertos, utilizaron unas herramientas robadas en agosto del año pasado a la NSA, la agencia de inteligencia norteamericana, difundidas luego por Wikileaks. Este tipo de agresiones se suelen lanzar por correo electrónico, por lo que se necesita que el usuario caiga la trampa y haga clic en un enlace; pero en este caso el virus penetraba por conexiones y puertos abiertos donde se comparten ficheros. Un ataque ideal para golpear a redes de ordenadores conectados entre sí, como empresas y oficinas gubernamentales.

El hacker argentino César Cerrudo explica que la digitalización hace que la sociedad progrese pero a la vez nos hace más vulnerables. Y el próximo, como mostró este ciberataque, podría afectar a cualquier sistema: Gobiernos, empresas, hospitales, sistemas de justicia. Cualquier dispositivo conectado a Internet corre el riesgo de ser asaltado. Estaríamos ante un futuro con tintes apocalípticos. El propio Cerrudo y un compañero demostraron hace poco que podían controlar robots, que en unos años formaran parte de nuestra vida como los móviles o las tablets. “En la siguiente generación los asistentes personales como Siri tendrán cuerpo y podrán moverse. Imagínate poder controlarlos desde fuera”, reflexiona en voz alta.

La primera llamada de un afectado que recibe en el Centro Criptológico Nacional español, un organismo adscrito al Centro Nacional de Inteligencia (CNI), fue del departamento de seguridad corporativa de Telefónica. En la misma situación están compañías automovilísticas, bancos y ministerios de medio mundo, aunque la mayoría lo oculta. Son las 10.30. Luis, que en ese momento ya ha llamado a su pareja diciéndole que se frustra el viaje, pide una copia del virus para que puedan analizarlo. Al recibirlo y ejecutarlo en una de sus máquinas, comprueba que se trata de un malware común, sin un desarrollo muy complejo. Lo novedoso es su indetectabilidad, opaco para el 60% de los antivirus. Poco después, desde Londres se ponen en contacto con ellos para preguntarles si saben lo que está ocurriendo. Los informáticos españoles les envían de inmediato una copia de WannaCry.

Ante una crisis de este tipo no existe el Brexit. El ciberataque afecta al servicio nacional de Salud (NHS, por sus siglas en inglés), con repercusión directa en 16 hospitales y centros de salud. La primera ministra, Theresa May, asegura que no hay indicios de que la información de los pacientes haya sido “comprometida”, y es cierto.

El virus no roba datos, los encripta y con el paso del tiempo los destruye. Sabina Moreno, de 33 años, acude en metro a su cita en el hospital Mile End, que pertenece al Royal London. Desde hace cuatro años sufre unos dolores terribles de espalda y cuello debido a las horas que ha pasado trabajando frente a un ordenador en mala posición. A eso hay que sumarle el estrés de ser madre y dueña y única trabajadora de su empresa de venta de bañadores para bebés. Al llegar, se encuentra al recepcionista sepultado en un mar de papeles. Son las citas de los pacientes, imprimidas y anotadas a mano. En la sesión la fisioterapeuta le dice que no puede acceder al historial ni al resultado de las pruebas que se había hecho la semana pasada. El sistema ha retrocedido un par de décadas.

WannaCry ha tenido más víctimas de las declaradas. Muchas firmas prefieren ocultar el bochorno de quedar expuestas a merced de los atacantes que pasar por el escarnio de ser vulnerables por no ejecutar un sencillo y rutinario parche de Windows. La aseguradora de riesgos digitales estima el coste potencial del ataque en 4.000 millones de dólares. Una cifra notable si se tiene en cuenta que en todo 2016 valoró en 1.500 millones de dólares las pérdidas generadas por ataques.

Marcus Hutchis, el británico de 22 años que consiguió aplacar a WannaCry.

Sin embargo, siguiendo las tres cuentas abiertas para recibir el dinero del rescate, lo recaudado apenas supera los 100.000 dólares. “Con el revuelo que se ha creado va a ser difícil que cobren. Les caerían encima policías y servicios secretos de todos lados”, añade Eusebio Nieva, director de Check Point en España y Portugal. La desproporción entre los daños causados y la cantidad recaudada por los hackers invita a dos reflexiones. Primera, que puede que no sea grandes profesionales o que, si se confirma la tesis de que el ataque está impulsado por Corea del Norte, como creen muchos forenses digitales ya que tiene similitudes con el pirateo a Sony, el fin último del ataque no era lucrativo. ¿En realidad querían probar su potencia de tiro?

En otro punto de Inglaterra, en el condado de Devon, a un chico de 22 años se le enciende una bombilla. Marcus Hutchins encuentra un dominio oculto en el virus, lo compra por 10 dólares y logra apagarlo creando un interruptor. Bingo. Funciona. El truco de Hutchins libera a miles de ordenadores de la infección. Mientras tanto, los informáticos españoles analizan el bicho, como comienzan a llamarle con familiaridad. Luis está convencido de que no ha sido diseñado para ganar dinero, es poco sofisticado en ese sentido. Con su equipo, hace ingeniería inversa, es decir, descubrir cómo funciona.

Se crea un gabinete de crisis improvisado. Luis y sus muchachos van en vaqueros y llevan camisetas negras con lemas de juegos de rol y competiciones de hackers. Los jefes, miembros de la Administración, en traje y corbata. Juntos encuentran otra forma de engañar al virus. Estos suelen traer un Mutex, un dispositivo que avisa al propio virus malware de que ya está ejecutado en un ordenador y no lo

1. Ataques en la red

"Un ataque es un evento exitoso o no, que atenta sobre el buen funcionamiento del sistema. En el flujo normal de la información no debe existir ningún tipo de obstáculos para que la información llegue al destinatario."[7]

De acuerdo con Symantec, existe un indicador que evalúa la actividad del malware y, por cuanto hace a los países en la región de América, ésta es una de las zonas donde se llevan a cabo o tiene su origen la mayor cantidad de actividad maliciosa a nivel mundial.

Al estudiar los ataques en la red descubrimos distintos temas que rondan sobre el mismo:

1.– La naturaleza del ataque. El tipo de código malicioso
2.– El lugar de origen. El lugar de destino o su dispersión incontrolada.
3.– El autor o los autores del ataque
4.– La vulnerabilidad de los equipos atacados
5.– La información que se pierde o que es motivo de un cifrado no autorizado.
6.– La legislación que protege dicha información. Y que ésta esté homologada a nivel internacional.
7.– Que la información retenida sirva como precursora para otro tipo de conductas delictivas como la extorsión.

Si queda descuidado alguno de estos aspectos, el resultado es evidente, se abre la puerta a la impunidad y por tanto a que se sigan replicando esta clase de conductas.

La actividad maliciosa, se describe en la página de la empresa dedicada al combate de códigos maliciosos[8], suele afectar a computadoras que se conectan a Internet mediante banda ancha de alta velocidad dado que estas conexiones son objetivos atractivos para los atacantes.

Estas conexiones ofrecen mayor capacidad de ancho de banda que otros tipos de conexión, mejor velocidad, la posibilidad de contar con sistemas continuamente conectados y generalmente una conexión más estable. Symantec clasifica las actividades maliciosas de la siguiente manera:

- **Código malicioso** - Incluye virus, gusanos y Troyanos que se introducen en forma oculta dentro

haga dos veces para no interferir. Activando el Mutex en una máquina sin infectar consiguen que el malware se dé media y vuelta no vuelva. Es una solución momentánea, socorrida. "Pero sucia, puede crear problemas", reflexiona Luis.

En un edificio del barrio de Chamberí hay una casa sin luz. Es la de José María, el único de su bloque que está a oscuras. Llama a su hija para que hable con la compañía y lo arreglen lo antes posible. La mujer llama y se encuentra a una teleoperadora nerviosa y desbordada. Le toma los datos a mano y le dice que en algún momento irán a solucionarlo pero que ahora mismo no puede hacer nada. "No podemos usar los ordenadores y esto de mandar físicamente a alguien no se hace desde hace muchos años", le cuenta al otro lado del teléfono. Mandar a un técnico, como ocurría hace bien poco, parece ahora antediluviano.

La solución de urgencia se perfecciona en Madrid 24 horas después, al margen del parche de Microsoft. El equipo del CCN cuelga una nueva versión perfeccionada del programa, algo muy sencillo, que no tiene más de 60 líneas de código. En los próximos días será descargado 50.000 veces. Tras escanear todas las Ip de España, todavía ven que hay más de 2.000 ordenadores en riesgo, pero poco más se puede hacer. Los informáticos, de todos modos, también crean soluciones a medida. Hay empresas españolas con sistemas operativos tan antiguos, como Windows 2000, que no pueden hacer nada para retomar su producción. Luis busca una versión en farsi de 1997, la prehistoria tecnológica. En los foros de Internet hay quien empiezan a alertar de que instalar ese parche supondrá abrir de par en par tu privacidad al servicio secreto. En esos círculos donde abunda la sospecha no son muy populares. Luis los lee y se rie. El trabajo está hecho. **Madrid / San Francisco** 22 MAY 2017 - 08:44 CDT Consultado en: https://elpais.com/internacional/2017/05/20/actualidad/1495291083_920693.html 10 de enero de 2018, 16:48 hs.

7 http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Ataques.php

8 Las amenazas de código malicioso se clasifican en cuatro tipos principales - puertas traseras (backdoors), virus, gusanos y Troyanos:

■ **Puertas traseras (backdoors)** - Permiten que un atacante acceda en forma remota a computadoras afectadas.

■ **Troyanos** - Son código malicioso que los usuarios instalan en sus computadoras sin darse cuenta, por lo general abriendo adjuntos de correo electrónico o realizando descargas desde Internet. Habitualmente, es otro código malicioso el que descarga e instala el troyano. Los programas troyanos difieren de los gusanos y los virus porque no se propagan por sí mismos.

■ **Virus** - Se propagan mediante la infección de archivos existentes en computadoras afectadas con código malicioso.

■ **Gusanos** - Son amenazas de código malicioso que pueden replicarse en computadoras infectadas o de algún modo que facilite su copia a otro equipo (por ejemplo, a través de dispositivos de almacenamiento USB).

Muchas amenazas de código malicioso tienen múltiples características. Por ejemplo, una puerta trasera siempre se encuentra junto con otra característica de código malicioso. Normalmente, los backdoor también son Troyanos; no obstante, muchos gusanos y virus también incorporan la funcionalidad de puerta trasera. Además, muchas muestras de código malicioso pueden clasificarse como gusano y como virus debido al modo en que se propagan. Una de las razones de esto es que los desarrolladores de amenazas intentan activar el código malicioso con múltiples vectores de propagación para aumentar las probabilidades de afectar con éxito a las computadoras durante los ataques. Fuente: https://www.symantec.com

de los programas. Entre los objetivos del código malicioso se encuentran la destrucción de datos, la ejecución de programas destructivos o intrusivos, el robo de información confidencial o sensible, además de poner en peligro la seguridad o integridad de los datos informáticos de la víctima.

- **Zombies de Spam** - Se trata de sistemas afectados que se controlan de manera remota y se utilizan para enviar grandes volúmenes de correo electrónico basura o no deseado (spam). Estos mensajes de correo electrónico pueden utilizarse para transmitir código malicioso y/o realizar intentos de phishing.
- **Hosts de phishing** - Un host de phishing es una computadora que ofrece servicios como aquellos de los sitios web para intentar obtener en forma ilegal información confidencial, personal y financiera simulando que la solicitud proviene de una organización confiable y reconocida. Estos sitios web están diseñados para simular los sitios de empresas legítimas.
- **Computadoras infectadas por bots** - Se trata de computadoras que han sido comprometidas y cuyos atacantes las controlan de manera remota. Habitualmente, el atacante remoto controla una gran cantidad de equipos afectados por medio de un canal único y confiable en una red de bots (botnet) que luego se utiliza para lanzar ataques coordinados.
- **Orígenes de los ataques a redes** - Se trata de las fuentes que dan origen a los ataques por Internet. Por ejemplo, los ataques pueden dirigirse a vulnerabilidades de protocolos SQL o desbordamiento de búfer.
- **Orígenes de ataques basados en web** - Mide las fuentes de ataques que llegan a través de la Web o por HTTP. Por lo general, esto afecta a sitios web legítimos que se utilizan para atacar a visitantes desprevenidos[9].

¿De qué manera se han evitado los ataques en la red? Bien por una adecuada protección física o lógica, por no ser objeto de los ataques o, pareciera irreal, pero por estar desconectado de la red por una suerte más de carácter generacional que por un criterio de prevención[10].

En la legislación penal española, los ataques en la red no están regulados de manera explícita, sino como una

9 Confróntese tanto la página de Symantec.com, como los estudios que anualmente publica para dar cuenta del número y dimensión de los ataques en la red, así como el origen y destino de los ataques.

10 Joel Gómez Treviño describe otro tipo de ataques en la red:

DoS es la abreviatura en inglés de Ataque de Denegación de Servicios, y DDoS corresponde a Ataque Distribuido de Denegación de Servicios. Richard Power, en su libro Tangled Web, Tales of the Digital Crime from the Shadows of Cyberspace, nos ayuda a comprender las diferencias y objetivos de estos ataques:

1. El objetivo de un **ataque de denegación de servicio (DoS)** es hacer inoperable a un sistema (computadora). Algunos ataques de denegación de servicio están diseñados para bloquear el sistema de destino, mientras que otros sólo tienen por objeto provocar que el sistema de destino tan ocupado que no pueda manejar su carga normal de trabajo.

2. En un **ataque distribuido de denegación de servicio (DDoS)**, un atacante puede controlar decenas o incluso cientos de servidores y apuntar toda esa potencia de ataque acumulada de todos estos sistemas a un único objetivo (servidor o computadora). En lugar de lanzar un ataque desde un único sistema (como sucede con el DoS), el atacante irrumpe en numerosos sitios, instala el *script* del ataque de denegación de servicio a cada uno, y luego organiza un ataque coordinado para ampliar la intensidad de estas agresiones cibernéticas. A este método suele conocérsele como "El Ataque de los Zombis", el cual dificulta a los investigadores forenses el rastreo de la fuente real del ataque.

A la definición de Power de DDoS debo agregar que otra opción es que el atacante solicite la colaboración de decenas, cientos o miles de personas para que cada una de ellas desde sus respectivas trincheras (computadoras) inicie el ataque simultáneamente contra un solo objetivo; lo que más adelante, dentro del presente estudio, se presentará con el concepto de "hacktivismo".

El DoS es un ataque "uno contra uno" y el DDoS es un ataque de "muchos contra uno". En términos generales, se dice que el objetivo de estos ataques regularmente es "tumbar un sitio web" (o más bien el servidor que responde a éste) enviando una gran cantidad de peticiones (paquetes de información) al servidor hasta que este se vuelva incapaz de responderlas. De ahí el nombre "denegación de servicios". [ ]

Un ataque de denegación de servicios (distribuido o no) puede llevarse a cabo de muy diversas maneras. En cierto tipo de ataques, un saboteador puede tirar un servidor remotamente sin necesidad de tener acceso al objetivo. Como lo comentamos con anterioridad, esto normalmente involucra el "inundar" el servidor con largos paquetes o un gran número de paquetes que el servidor no está preparado para manejar.

Algunos ejemplos de métodos tradicionales o "históricos" para lograr una denegación de servicio son: 1) el ping de la muerte, 2) *smurfing* o *ping flooding*, 3) SYN *flooding* y 4) *teardrop*, etc. Otra posibilidad es crear scripts o pequeños programas y ponerlos a disposición de la "comunidad hacktivista" (subirlos a sitios web para su descarga y/o ejecución masiva) para realizar ataques distribuidos de denegación de servicios (DDoS).

consecuencia del acceso no autorizado. En particular, el artículo 197 bis prevé:

"**Artículo 197 bis.**

1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses."

Por cuanto hace a la legislación mexicana, cuyo texto no ha cambiado sustancialmente desde que se incorporó al texto penal federal establece:

"Artículo 211 bis 1.– Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa."

Sobre este artículo y, atendiendo a la naturaleza de los ataques de reciente cuño, debemos señalar la ausencia de la fórmula "limite o condicione el acceso".

2. Hackers

La denominación de hacker ha tenido una evolución, desde contemplarlos como piratas cibernéticos hasta develar su naturaleza como personas con habilidades para detectar la vulnerabilidad de los equipos y cuya actividad no es sinónimo de delincuente informático, salvo que su conducta esté enfocada de manera dolosa a detectar y aprovechar la vulnerabilidad de los equipos.

Entre las conductas previstas desde hace ya varios años por la Organización de las Naciones Unidas, está el llamado Acceso no autorizado a servicios y sistemas informáticos. Es el acceso no autorizado a sistemas informáticos por motivos diversos: desde la simple curiosidad, como en el caso de muchos *hackers* hasta el sabotaje o espionaje informático.

El acceso se efectúa, en teoría, desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los *hackers* se hacen pasar por usuarios legítimos del sistema[11]; esto suele suceder con frecuencia en los sistemas en los que los usuarios

---

Tal vez el más famosos de estos programas es el denominado "*Flood Net*", creado en 1999 por un grupo de hacktivistas llamado "*The Electronic Disturbance Theater*", para apoyar la causa del Ejército Zapatista de Liberación Nacional en Chiapas, México. Cuando abordemos el entorno sociopolítico, comprobaremos que México ha tenido episodios de fama mundial en lo que a hacktivismo y ataques de denegación de servicio se refiere.

Este tipo de ataques no representan un *hackeo* tradicional, es decir, no hay intrusión o vulneración de una computadora por acceso no autorizado. El agresor no tiene acceso a los archivos o información personal contenida en el servidor o computadora objetivo del ataque. (*El Derecho en la era digital*, 1ª ed., Porrúa, (coord. Alberto Enrique Nava Garcés, México, 2013, pp. 48 -50)

11 "Hackers, genios que se desligan del hampa". Saben de lo que son capaces y por eso temen que la delincuencia organizada los obligue a trabajar para ellos. En la mente de un hacker siempre existe un reto informativo. Buscan, investigan, leen, se documentan, practican, exploran, prueban hasta que lo vencen. Su naturaleza es encontrar vulnerabilidad en sistemas operativos, en páginas web, además de identificar deficiencias en seguridad informática. Son toda una comunidad que comparte gustos, cultura y habilidades. Magos de las redes y programadores expertos.

Los hackers han construido Internet. Han creado softwares gratuitos. Han facilitando el acceso a la información y a los recursos de computación mientras les ha sido posible. Por naturaleza son curiosos, perspicaces y un poco paranoicos. Los hay desde los 15 hasta los 45 años. No tienen un mismo modelo de vestimienta ni comparten actitudes, aunque si aptitudes y generalmente hacen públicas sus habilidades en la red, algunos famosos, sólo porque gracias al nick que utilizan se identifican los retos que pudieron vencer o se sabe para qué habilidad son buenos.

Pekka Himanen, Linus Torvalds y Manuel Castells los definen en su libro La ética del hacker y el espíritu de la era de la información como personas que se dedican a programar de forma entusiasta y que comparten información elaborando software gratuito y facilitando el acceso a la información. Separan a aquellos que dedican su tiempo a escribir virus informáticos y a colarse en los sistemas de información, "los hackers empezaron a denominar crakers a estos usuarios destructivos o piratas informáticos que enfocan sus esfuerzos en tres rubros: el mercado de fraudes con automóviles; fraudes con créditos, ya sea tarjetas departamentales o tarjetas de crédito y al lavado de dinero".

Raza mexicana

KIOSKO entrevistó a tres auténticos hackers, todos integrantes de Raza Mexicana, una de las comunidades más sólidas donde los hackers comparten gustos y habilidades en la red.

Dicen estar cansados de que los medios saquen conclusiones diparatadas y sin fundamento que generalizan o etiquetan a estas comunidades.

pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema[12].

Aseguran que no es culpa de ellos que en Tepito se vendan bases de datos. “No robamos información para luego venderla al mejor postor, en este caso no existen pruebas de que alguien haya ingresado ilegalmente a los servidores donde se supone estos datos estaban resguardados; hay problemas que se explican más con la corrupción que con la vulnerabilidad de los sistemas”, dicen.

Son conscientes de que pueden encontrar errores de seguridad informática en casi cualquier cosa que se maneje con un sistema operativo.

“Es verdad que se pueden cambiar calificaciones de una universidad o hablar gratis desde un celular o hacerle creer a un sistema operativo que se pagó un recurso, hasta tirar aviones o descomponer el Metro, pero el mismo alcance tiene un niño con una AK-47, un lanzacohetes puede derribar un avión y un empleado del Metro puede provocar premeditadamente un choque de trenes. A un hacker le interesa comprender y probarse en un ambiente controlado”, dicen.

Aseguran no ser más de 20 con buen nivel. “Buenos, muy buenos, no rebasan los 20 y de habilidades estándar existen unos 500 en todo el país, no más”.

Explican que desean estar en el anonimato, pues sus habilidades correrían peligro si el crimen organizado tuviera idea de lo que con sus retos informativos pueden lograr. Algunos son expertos en web, otros en seguridad de software, y otros que encuentran vulnerabilidad a nivel protocolo, como en FTP.

Las clasificaciones y la seguridad

Dicen estar interesados en demostrar que las protecciones que le ponen al software son vulnerables. “Hemos encontrado fallas en sistemas de correo electrónico, en Telmex en aplicaciones comerciales de software y hemos obtenido licencias gratuitas”.

En el mundo de los hackers hay clasificaciones: los de sombrero blanco buscan crear con lo que descubren; los de sombrero gris generalmente buscan beneficios económicos con las vulneravilidades que encuentran y los de sombrero negro, catalogados como delincuentes cibernéticos que ayudan al narco, al plagio o a robar información de empresas para venderla a la compañía contraria.

Dicen que, aunque la seguridad cibernética en México está en pañales, aunque va en aumento, pues ha crecido mucho en los últimos años, sobre todo en instituciones bancarias y tiendas departamentales. “Aún hay fallas, pero se ha avanzado en el tema”, aseguran.

Esa es una buena noticia, pues a pesar de que México tiene un mercado potencial de transacciones a través de Internet superior a los 14 mil 300 millones de dólares anuales, las operaciones sólo llegan a 17.7%, es decir, 2 mil 384 millones, principalmente por el temor de los usuarios al fraude.

Las cifras tampoco ayudan a generar confianza entre los usuarios. Durante 2006, el fraude cibernético ascendió a 7 mil millones de pesos, que se perdieron por tres situaciones: ayuda de delincuentes cibernéticos, fallas en los sistemas de seguridad de las instituciones y desconocimiento de medidas de seguridad para realizar transacciones a través de Internet por parte de los usuarios.

Según la Asociación Mexicana de Internet (Amipci), 31% de los 3.4 millones de usuarios del servicio en el país desconocen las medidas de seguridad y 14% no saben como usarlas.

En las cárceles del país aún son pocos los delincuentes que pagan condenas por fraudes cibernéticos, uno de los casos más conocidos es el de un joven de 20 años que logró transferir 3 millones 612 mil 500 pesos del banco a su cuenta personal. Experto en sistemas, Ricardo Reyes Orozco vulneró los sistemas de bancanet de Banamex.

Logró retirar 526 mil pesos, cobrando 29 cheques en diferentes días en distintas sucursales del banco. Hoy está preso en el Reclusorio Sur por su hazaña. (consultado en https://www.elsiglodetorreon.com.mx/noticia/519765.hackers-genios-que-se-desligan-del-hampa.html 10 de enero de 2018 16:14hs).

12 **Desmantelan red de hackers en España**. **Los hackers son responsables de extraer más de 60 mdd en el mundo**. Una operación conjunta de la **Policía Nacional española** y una agencia de seguridad estadunidense permitió desmantelar la rama española de una red de hackers responsable de extraer más de 60 millones de dólares en cajeros de todo el mundo.

En la operación fueron detenidas ocho personas, dio a conocer el Ministerio español del Interior.

Señaló que esta red actuó el pasado febrero de forma simultánea en 23 países y en pocas horas se hicieron con 40 millones de dólares en 34 mil retiros de efectivo.

Precisó que 446 de esas disposiciones de efectivo se realizaron en una sola noche en cajeros de Madrid, donde la rama española de la organización obtuvo cerca de 400 mil dólares.

Explicó que los ocho detenidos en Madrid seguían precisas instrucciones del líder de la red, un experto informático arrestado en **Alemania** capaz de vulnerar las bases de datos de entidades bancarias para inhabilitar todas las medidas de seguridad y restricciones sobre el uso de tarjetas.

Anotó que la estructura de esta red mundial nacía de una sola persona, quien definía las relaciones a mantener por el resto de miembros y el momento preciso en el que activarlos para obtener la mayor cantidad de efectivo en el menor tiempo posible.

Este líder era capaz de atacar las bases de datos de compañías procesadoras de los datos de tarjetas de crédito de las entidades bancarias para robar información altamente sensible.

Cuando lograba comprometer el sistema, tenía acceso a inhabilitar todas las medidas de seguridad, incluyendo restricciones de velocidad, restricciones geográficas, restricciones de balance (permitiendo realizar transacciones con balances negativos) y hasta restricciones del PIN (permitiendo a los autores incorporar cualquier PIN).

Apuntó que para llevar a la práctica la estafa, el cerebro de la red comunicaba determinadas numeraciones de tarjetas bancarias a personas de su confianza repartidas por todo el mundo.

III. EL CASO SNOWDEN

Las nuevas tecnologías de la información han rebasado por mucho la ficción con la que han sido concebidas y, en muchas ocasiones, han cumplido vaticinios sobre el mal uso de las mismas.

La historia de Edward *Snowden* es la de un ex espía de las grandes instituciones como son la NSA (Agencia de Seguridad Nacional) y la CIA (Agencia Central de Inteligencia) creadas en Estados Unidos para la seguridad interior y la vigilancia de "los enemigos" y cuya deserción provocó una persecución mundial debido a la divulgación de las tareas de espionaje que realiza aquella potencia contra sus propios ciudadanos y contra los que se supone son los países aliados.

Edward Snowden fue un empleado de las instituciones especializadas en seguridad e inteligencia de los Estados Unidos de América. Su caso fue la secuela de otro similar conocido como *Wikileaks*, mediante el cual se dio a conocer al público diversos documentos confidenciales que exponían el trabajo que se realizaba desde la diplomacia para hacerse de información privilegiada.

Aquel primer escándalo le costó la persecución y el asilo político forzado a Julian Assange. Pero, a diferencia de aquél, Snowden era norteamericano y sabía, por haber estado dentro del gobierno hasta dónde llegaba su intrusión en las comunicaciones privadas.

Sin embargo, y con la amenaza de ser acusado de delitos muy graves y de ser perseguido con más ferocidad por el Estado vigilante, Snowden aportó los elementos para exhibir al gobierno de los Estados Unidos y sus prácticas de vigilancia hacia sus propios ciudadanos en franca violación a sus libertades.

Como es de suponer, Snowden quedó atrapado en ese limbo en el que la ética lo contrapone con las leyes de su país y, a pesar de sus fines, tuvo que huir hacia un estado protector, tradicionalmente antagónico como es Rusia.

IV. LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN Y EL DERECHO PENAL

La historia se relaciona con el derecho penal por los bienes jurídicos en conflicto, al revelar la violación institucional de la intimidad de todos los usuarios de las comunicaciones y lo que implica realizar actos como la revelación de secretos que importan la seguridad del Estado. Así también hay una relación con la responsabilidad de los aparatos organizados de poder que, de manera institucionalizada y bajo la simulación de actos jurídicos invaden la privacidad de todos los gobernados.

Así, quedan de manifiesto el uso que se le da a la *Ley de Vigilancia de la Inteligencia Extranjera de 1978* (EEUU) y al Tribunal secreto, *El Tribunal de Vigilancia de Inteligencia Extranjera de los Estados Unidos de América,* que se instituyó con el fin de legalizar las intervenciones de comunicaciones.

Y a pesar de que se dice que, a consecuencia del caso Snowden ya no existe tal intrusión, el caso *Silk road*, deja en claro que tal vez ya hubo una respuesta gubernamental que no ha sido debidamente acatada[13]. Las

---

Los líderes de cada célula copiaban estas numeraciones en tarjetas blancas dotadas de bandas magnéticas y las distribuían entre su red de colaboradores.

En el momento exacto en el que el líder eliminaba los límites de retiro y restricciones geográficas de estas tarjetas comenzaba una operación coordinada a escala mundial para extraer en cajeros automáticos y de forma simultánea la mayor cantidad de efectivo disponible.

El Ministerio español del Interior resaltó que **Estados Unidos** investigaba desde el año 2007 las actividades ilícitas de una compleja organización involucrada de forma regular en actividades de extracción de efectivo en cajeros automáticos.

Las investigaciones desarrolladas en Estados Unidos permitieron la identificación y posterior desarticulación a principios de mayo de la célula encargada de realizar las operaciones en la ciudad de Nueva York, compuesta por ocho individuos.

Siete de ellos fueron detenidos y el octavo, supuesto líder de la célula, habría sido asesinado en República Dominicana el pasado 27 de abril.

Por su parte, los investigadores españoles lograron identificar a las personas que formarían la célula de la organización asentada en España.

Precisó que ocho personas fueron finalmente detenidas, seis de nacionalidad rumana y dos naturales de Marruecos, en las localidades madrileñas de Mejorada del Campo y Fuenlabrada.

Además se practicaron tres registros domiciliarios en los que se decomisaron 25 mil euros en efectivo, dos lectores grabadores de tarjetas de crédito, alrededor de mil tarjetas vírgenes con banda magnética, material informático, y gran cantidad de joyas y documentación pendiente de análisis.

Asimismo, se han asegurado dos inmuebles valorados en más de 500 mil euros. (Notimex El Universal 05:44 Madrid | Domingo 29 de diciembre de 2013).

13 Internet anónimo. "El Deep Web es un sitio perfecto para el crimen organizado. Ahí pueden establecerse contactos que no son monitoreados, nadie está allí observando. Además, las transferencias tanto de mercancías como de pagos son prácticamente imposibles

tecnologías han avanzado demasiado como para dejar de ser utilizadas, por ejemplo, los detectores de retina, las cámaras que se prenden de manera remota, los vehículos de conducción totalmente automática, etcétera.

Los *hackers*, autores de los ataques en cuestión, como estarán definidos líneas abajo, poseen habilidades que, sus propios colegas aprenden y pueden resolver. Por eso, muchas veces se piensa que la tecnología y su avance no puede ser detenido solo con el marco de la ley sino con la propia tecnología.

A los hackers de alguna potencia mundial, se les contiene con *hackers* de otra potencia. En ese contexto debemos preguntarnos ¿dónde y quién recluta en nuestro país a los especialistas para contener ataques cibernéticos? Existen los denominados CERT que son el Equipo de Respuesta a Incidentes de Seguridad en Cómputo[14]. Este equipo es capaz de atender incidentes de cómputo, realizar análisis de vulnerabilidades, pruebas de penetración, cómputo forense, además de investigación relacionada con la seguridad informática. Entre otros, destacan el INCIBE (Instituto Nacional de Ciberseguridad de España) o el CERT de la Universidad Nacional Autónoma de México[15].

---

de rastrear. Ahí tenemos el emblemático caso de Silk Road", señaló Carlos Chalico, experto en seguridad informática y académico de la Universidad de Toronto.

El caso que menciona Chalico fue el que llamó la atención global sobre el fenómeno del Internet Profundo. Silk Road fue un sitio alojado en Deep Web en el cual se traficaba con drogas como Heroína, LSD y Cannabis, principalmente. Abierto en 2011 y cerrado en 2013 por el FBI, los vendedores y consumidores de Silk Road pudieron pasar inadvertidos para el público en general gracias a que las transacciones se pactaban con ciertos horarios y los pagos se realizaban vía Bitcoin, una criptomoneda imposible de rastrear.

Su fundador, conocido como "Dread Pirate Roberts" fue identificado por el FBI como Ross William Ulbricht y sentenciado en 2015 a cadena perpetua, al encontrase culpable de siete cargos federales como contrabando y conspiración.

México también está en la internet profunda. No solamente criminales estadounidenses o europeos utilizan la Internet Profunda, en México esta plataforma tiene un uso bastante diverso.

En 2014, el país participó en la Operación "Sin Fronteras", que detuvo a una red de pornografía infantil en 14 países de América Latina y Europa. Muchos de sus miembros operaban al cobijo de Deep Web.

Un informe de la División Cibernética de la Policía Federal asegura que dicha unidad ha identificado actividad ilícita en temas relacionados a pederastia, trata de personas y narcotráfico, aunque por la naturaleza de la plataforma no puede identificar el origen de esta actividad.

No es algo que sorprenda, señaló Derek Manky, "los criminales preferirán siempre aquella infraestructura que les permita operar sin ser vistos. México actualmente se encuentra en tercer lugar como país que provee servidores y redes TI para realizar ataques maliciosos. Por tanto es natural concluir que el crimen organizado, nacional y extranjero está aprovechando esta circunstancia para explotar los beneficios del Deep Web".

Pero el anonimato que ofrece la Internet Profunda no solamente es buscado por grupos delictivos, también representa la única opción para mexicanos que encuentran en la oscuridad de esta plataforma el lugar ideal para escapar de circunstancias que atentan contra su vida.

"Sabemos que la Deep Web en México también es utilizada de manera importante por los periodistas para realizar sus investigaciones y por representantes de organizaciones sociales y civiles; el carácter secreto del Deep Web les permite desaparecer del mapa", señaló Carlos Chalico. (Consultado en

http://www.eluniversal.com.mx/articulo/techbit/2016/07/28/conoce-la-web-fondo 10 de enero de 2018, 16:24 hs).

14 Gustavo Eduardo Aboso escribe: "El espacio virtual se ha transformado desde hace tiempo en un terreno fértil para la lucha cibernética entre los países en el marco de una guerra no declarada. Los *hackers* de uno y otro bando operan habitualmente contra los sistemas informáticos del contrario, testeando su capacidad de seguridad y aprovechando sus brechas para cometer espionaje industrial, comercial y militar. En esa perspectiva, la cooperación internacional debe cerrar filas frente a esas conductas ilícitas que atentan contra la integridad, la confianza y el funcionamiento de los sistemas automatizados en la sociedad de la información". (*op. cit.*, p. 423.)

15 TheHackerNews 03/08/2017 Aunque la ola de los ransomware WannaCry y Petya se ha frenado, atacantes y cibercriminales han tomado notas de los brotes globales para crear *malware* más poderoso.

Investigadores de seguridad han descubierto al menos a un grupo de cibercriminales que está tratando de dar a sus troyanos bancarios las capacidades de propagarse automáticamente, similares a las de un gusano, que hicieron que los ataques de ransomware recientes llegaran a todo el mundo.

La nueva versión de troyano bancario TrickBot, conocido como "1000029" (v24), roba credenciales usando el protocolo Windows Server Message Block (SMB), el cual permitio a WannaCry y a Petya propagarse rápidamente por todo el mundo.

TrickBot es un troyano bancario que ha afectado instituciones financieras en todo el mundo desde el año pasado. El troyano generalmente se propaga a través de archivos adjuntos de correos electrónicos, intentando engañar a los usuarios haciéndose pasar por una "institución financiera internacional" sin nombre, que solicita las credenciales de la víctima usando una página de inicio de sesión falsa.

La semana pasada investigadores de Flashpoint, que han estado registrando continuamente las actividades de TrickBot y sus objetivos, han descubierto que el troyano ha evolucionado para propagarse localmente en las redes usando el Server Message Block (SMB). La nueva versión de TrickBot todavía está en pruebas, por lo que aún no están completamente implementadas las nuevas funciones. Tampoco

V. EL CONVENIO DE BUDAPEST

Entre los instrumentos internacionales que se han realizado en torno al tema de la ciberdelincuencia, destaca, aun cuando ya han pasado más de quince años desde su realización, el Convenio de Budapest contra la delincuencia informática, al cual, por la complejidad de las obligaciones para los países firmantes, México (a diferencia de España que firmó y se adhirió al referido tratado) se ha quedado solo para analizar su probable adhesión. Para entonces, si es que decide adherirse, lo hará a un instrumento obsoleto.

El Convenio de Budapest establece en sus artículo 4 y 5, la previsión contra los ataques en la red.

> Artículo 4.– Ataques a la integridad de los datos
>
> l. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.
>
> 2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo l comporten daños graves.
>
> Artículo 5.– Ataques a la integridad del sistema
>
> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro informáticos.

Aun cuando México ha sido omiso en la adhesión a este instrumento internacional, en la legislación interna se encuentran fórmulas que prevén la conducta típica.

VI. LA LEGISLACIÓN FEDERAL MEXICANA

En 1999 se incorporaron al Código penal federal 7 artículos para tipificar los delitos informáticos. Sin tener en claro el bien jurídico tuteado se establecieron bajo el capítulo de revelación de secretos y acceso ilícito a equipos de informática.

El hilo conductor de estas conductas se reduce a la introducción, acceso, modificación, destrucción, producir pérdida, conocer o copiar la información contenida en algún equipo o sistema de informática. La variación sobre la licitud precedente (si se tiene autorización para acceder o no), el sujeto pasivo que puede ser cualquier particular, alguna institución del sistema financiero o bien que se agrave si el sistema o equipo de informática pertenece al Estado y el establecimiento de sanciones que no son muy graves comparadas con otras establecidas en el mismo cuerpo punitivo legal, la cual será aumentada, según el último artículo si la información ha sido utilizada en provecho propio o ajeno. Pero, de todos estos elementos que podemos distinguir a la luz de los elementos del tipo ya vistos en capítulos anteriores, resalta uno que implica un verdadero reto para ingenieros en sistemas cuando no conocen derecho o a los propios abogados desconocedores de lo que pueda significar que el equipo o sistema esté protegido por un mecanismo de seguridad.

Si pudiéramos proponer la modificación a los artículos citados, estableceríamos los siguientes textos normativos:

---

tiene la capacidad de escanear aleatoriamente IP externas para buscar conexiones SMB, como lo hace WannaCry usando una vulnerabilidad llamada EternalBlue.

Los investigadores de Flashpoint dijeron que el troyano fue modificado para escanear los dominios de las listas de servidores vulnerables, usando la API de NetServerEnum de Windows, de esta forma pueden enumerar otros equipos de la red a través de LDAP (Lightweight Directory Access Protocol). La nueva versión de TrickBot también se puede disfrazar con el nombre "setup.exe" y enviarse a través de PowerShell para propagarse a través de la comunicación entre procesos, con lo que se descargarían nuevas versiones en las unidades compartidas.

Según los investigadores, el último descubrimiento de las nuevas versiones de TrickBot proporciona una visión de lo que los creadores del malware podrían usar en el futuro próximo.

"Flashpoint estima con moderada confianza que la pandilla detrás de TrickBot probablemente continuará siendo una fuerza formidable a corto plazo", dijo Vitali Kremez, director de investigación en Flashpoint.

"Aunque el módulo para brindar propiedades de gusano actualmente parece poco desarrollado, es evidente que los creadores de TrickBot han aprendido de los brotes globales de ransomware con propiedades de gusano como WannaCry y 'NotPetya', y están intentado replicar su metodología". Consultado en https://www.seguridad.unam.mx/troyano-bancario-copia-propagacion-de-wannacry el 14 de enero de 2018, 18:26 hs.

Acceso ilícito a sistemas y equipos de informática
Artículo ---.– A quien sin autorización modifique, impida el acceso o limite este, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de uno a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de uno a dos años de prisión y de cincuenta a ciento cincuenta días multa.
Artículo ---.– A quien sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. A quien sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y de quinientos a mil días multa. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes. **Artículo ---.–** A quien estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. A quien estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.
A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública. **Artículo ---.–** A quien sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de instituciones bancarias o de aquellas que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
A quien sin autorización conozca o copie información contenida en sistemas o equipos de informática de instituciones bancarias o de aquellas que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. **Artículo ---.–** A quien estando autorizado para acceder a sistemas y equipos de informática de de las instituciones bancarias o de aquellas el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. A quien estando autorizado para acceder a sistemas y equipos de informática de instituciones bancarias o aquellas que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones bancarias o de aquellas que integran el sistema financiero. **Por mecanismo de seguridad se entenderá toda herramienta o técnica física o lógica, material o virtual, que sirva para preservar la confidencialidad, la integridad, y la disponibilidad de la información, para impedir el acceso libre a datos o información contenida o para salvaguardar algún bien informático.** **Artículo ---.–** Para los efectos de este capítulo, no se podrá argumentar que el equipo del que se obtenga la información cuente con puertos abiertos. **Artículo ---.–** Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno. Así lo hemos propuesto en el proyecto de Código Penal Nacional al que fuimos convocados por la Honorable Junta de Gobierno del Instituto Nacional de Ciencias Penales en noviembre de 2017.

VII. AUTORÍA Y COAUTORÍA

Por cuanto hace a la autoría en los ataques a la red, según lo establece el artículo 13 del Código penal federal (México):

> **Artículo 13**.– Son autores o partícipes del delito:
> **I.– Los que acuerden o preparen su realización.**
> **II.– Los que los realicen por sí;**
> **III.– Los que lo realicen conjuntamente;**
> […]
> Los autores o partícipes a que se refiere el presente artículo responderán cada uno en la medida de su propia culpabilidad.
> Para los sujetos a que se refieren las fracciones VI, VII y VIII, se aplicará la punibilidad dispuesta por el artículo 64 bis de este Código.

La teoría del "dominio del hecho" fue iniciada por Welzel, quien consideraba al autor como "aquel que mantiene una condición, consciente del fin, del acontecer causal en dirección del resultado típico, es señor sobre la realización del tipo"[16]. Para Mir Puig, escribe Donna:

> sólo son autores aquellos causantes del hecho imputable a quienes puede atribuirse la pertenencia, exclusiva o compartida, del delito; de entre aquellos causantes, el delito pertenecerá como autor a aquel o a aquéllos que, reuniendo las condiciones personales requeridas por el tipo (delitos especiales) aparezcan como protagonistas del mismo, como sujetos principales de su realización. Y más tarde afirma: 'La autoría supone, pues, que el delito es imputable al sujeto como suyo, supone una relación de pertenencia. Esta pertenencia corresponde en primer lugar al ejecutor material individual al que puede imputarse al delito'. En segundo lugar al autor mediato. El hombre de atrás es aquí el único causante del delito al que puede imputársele como propio. En tercer lugar, la pertenencia del hecho es compartida por quienes se distribuyen partes esenciales del plan global de ejecución del delito (coautoría)[17/18].

La identificación del autor no es tarea sencilla en tratándose de delitos informáticos. Su complejidad está basada en el medio remoto utilizado, la posibilidad de que el resultado de la conducta se produzca en un tiempo distante al hecho que lo produce y en una locación distinta. Más allá de estos aspectos característicos del medio informático, lo cierto es que también hay una huella que puede seguirse hasta encontrar más que la propia máquina, al sujeto detrás de ella. Y si esta conducta se realiza por un previo acuerdo, lo que actualiza la coautoría, la complejidad aumenta para establecer las parcelas que le corresponden en ese actuar, la división de tareas y que pueda existir una imputación recíproca, en tanto lo que hace uno le es imputable al otro.

Así que ya sea de *un hacker* o *un cracker* (voz cada vez más en desuso), para el derecho penal, la relevancia la tiene el título de la imputación y por tanto, los requisitos con los que deba contar el autor para ser así considerado.

Más allá del pretendido anonimato, para la ley sustantiva penal, le resulta de especial importancia delimitar la actuación del sujeto, el dominio que tiene del acto, de modo tal que dependa de él la consecución o la interrupción del mismo.

Por cuanto hace al coautor, éste no es accesorio, ni hace una parte separada del hecho, lo consolida con su actuación. Por eso, en la práctica resultan muy interesantes los aspectos probatorios respecto del llamado "acuerdo previo de voluntades" así como el dominio que cada cual ejerce respecto del hecho imputado.

Súmese a lo anterior: la realización del hecho a distancia, con posibilidades de que la programación implique un resultado en otro tiempo y bajo el supuesto cobijo del anonimato, que más bien ocurre bajo el cobijo de lugares donde no existe ley sustantiva aplicable.

VIII. CONCLUSIONES

El ataque en la red puede provenir de particulares o bien, de empresas (personas jurídicas con fines de competencia económica) y hasta de los propios Estados, lo que rebasaría el ámbito de aplicación de la ley penal y sus fines pueden ser diversos. Desde la simple afectación de un equipo hasta llegar al preámbulo de una guerra en el ámbito virtual.

Wannacry, solo fue un ejemplo entre varios, de la dimensión que puede tener un ataque y la afectación global que puede causar.

La pregunta es ¿hasta donde el CERT o los CERTs en México podrán contener esta clase de ataques, sobre soto si recordamos que tanto el software que se tiene, como los programas para evitar intrusión en equipos son de origen extranjero y a veces proviene de sitios donde también se producen, paradójicamente, pero no casualmente, los ataques en comento.

16 Welzel, Hans, *Derecho Penal Alemán. Parte General*, Chile, 1987, p. 145.

17 Mir Puig, ob. cit., ps. 366/7., citado por Donna, Edgardo Alberto. *La autoría y la participación criminal*, Granada, Comares, 2008, p. 37.

18 Donna, Edgardo Alberto, Op. cit., *La autoría*..., p. 37.

A los tradicionales problemas de los que la dogmática penal se ha ocupado por cuanto hace a la autoría, se deben agregar: la realización del hecho a distancia, con posibilidades de que la programación implique un resultado en otro tiempo y bajo el supuesto cobijo del anonimato, que más bien ocurre bajo el cobijo de lugares donde no existe ley sustantiva aplicable.

Así también ha despertado la atención de la opinión pública el hecho que, a través de un ataque en la red propicie la incertidumbre del resultado electoral, lo que en países como México que deben invertir ingentes cantidades para mantener a salvo la credibilidad de los comicios sería o causaría una afectación de proporciones preocupantes[19/20].

19 **La PGR se previene ante hackers electorales.** Por **Manuel Espino Bucio.** La Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas (UICOT) de la PGR se creó en septiembre del año pasado y su titular, Marcos Rosales García, asegura que a pesar del poco tiempo en operación, están listos para apoyar al Instituto Nacional Electoral (INE), si así lo desea, en el blindaje de sus sistemas informáticos, que pueden ser blanco de grupos hacktivistas o hackers durante el proceso electoral.

En entrevista con EL UNIVERSAL, reconoce que el INE cuenta con un sistema de avanzada. Rosales García afirma que en esta materia no hay nada que sea 100% seguro, por lo que "si el INE nos requiere para proteger alguna de sus infraestructuras, por supuesto que lo haríamos".

Presume que en el último cuatrimestre de 2017, la Unidad de Investigaciones identificó y mitigó más de 289 incidentes de seguridad informática que afectaban tanto al sector público como privado.

En la sede de la Agencia de Investigación Criminal, el funcionario destaca la erradicación del virus informático denominado FALLCHILL, de origen norcoreano, en una operación conjunta con el FBI, como el principal logro de la unidad, con apenas cuatro meses de creada.

Su objetivo, expone, era "robar información que estaba almacenada en los equipos de cómputo. Muchas veces buscan la información financiera que les permita hacerse de algunos recursos. Si se hubiera instalado en una infraestructura sensible, en la que la información que se almacena es de carácter confidencial o sensible, pues es explotable para los grupos que desarrollan estos malware".

Recuerda que al "estar interconectados con todo el mundo, todos los riesgos que ocurran alrededor del mundo son riesgos que eventualmente podemos recibir en nuestro país, pero estar alertando sobre cuáles son los mecanismos de prevención, ayuda". Ante ello, reveló que está en marcha un operativo conjunto con Interpol por amenazas de posibles ataques contra la infraestructura tecnológica del país.

¿Cuál es la incidencia de delitos cibernéticos en México?

-Hemos operado diferentes acciones en contra del cibercrimen, realizamos un par de operativos coordinados por Interpol, en los que muchos países alrededor del mundo, particularmente de América Latina, hemos participado y obtenido resultados importantes en la desarticulación de grupos cibercriminales.

Es importante decir que en nuestro país no tenemos estadística relacionada con los delitos cibernéticos que nos permita medir cuál es el impacto real que tienen estas conductas en contra del ciberespacio mexicano y particularmente los usuarios que están en la red nacional.

¿Cuáles son los delitos que más cometen los ciberdelincuentes y que detecta la UICOT?

-Hemos tenido muchos casos de clonación de sitios oficiales por parte de grupos hacktivistas o de hackers, que buscan robar información de una persona o generar algún tipo de estafa creando páginas apócrifas.

Es el delito más común, pero también hay ataques por denegación de servicio distribuido. Esto último quiere decir que muchos equipos hacen solicitudes a un solo servidor y eventualmente queda fuera de línea. Hay una gran variedad de delitos y algunos, por las temporadas, pueden ser más recurrentes que otros.

¿Cuáles delitos aumentan y en qué temporada?

-Cuando hay muchas compras en línea, los fraudes al comercio electrónico aumentan.

¿Cuántos ataques cibernéticos han detectado?

-Los ataques cibernéticos dirigidos van en diferentes sentidos: el robo de información de los equipos y los que buscan afectar la infraestructura para dejarla fuera de línea.

Así también hemos tenido ataques a sitios gubernamentales, a empresas. Particularmente, el malware que recientemente identificamos y que logramos desactivar estaba alojado en una empresa de telecomunicaciones, entonces no es un tema exclusivo de las dependencias gubernamentales.

Si bien muchas veces pueden ser objetivos con fines políticos, hay otros que lo que buscan es hacerse llegar de algún recurso y lo obtienen de empresas privadas, no del gobierno.

¿Han detectado ataques de grupos de hacktivistas?

-Sí, por supuesto. En algunos de los operativos que hemos participado anteriormente, hemos logrado identificar a, por lo menos, un par de grupos hacktivistas, uno con origen en Perú y otro en África. Hemos dado parte a las autoridades de estos países y les hemos entregado toda la información que hemos podido recolectar, para que ellos a su vez continúen con las líneas de investigación que puedan sancionar todas estas conductas.

¿Cómo detectaron el virus informático de origen norcoreano?

-El Homeland Security Investigations y el FBI identificaron el año pasado que estaba circulando por la red un código malicioso, realizaron una investigación técnica con los datos que obtuvieron y definieron que un virus realizaba actividades como la de instalarse en un equipo de cómputo.

Definieron un análisis técnico e identificaron que se distribuía en diferentes países y ubican que la información que se filtraba de los equipos que ya habían sido víctimas, se dirigía a una red con origen en Corea del Norte, por eso es que logran determinar el origen de estos códigos maliciosos.

El FBI dio parte a la PGR de que este virus podría estar en la red nacional, por lo que la unidad se puso a investigar y logró identificar que existían algunos servidores que habían sido comprometidos y nos pusimos en contacto con la empresa para hacerle saber la situación que tenía y tomar las medidas para que el virus no se siguiera propagando.

¿Cuál era la intención de ese malware en los equipos?

-Robar información que estaba almacenada en los equipos de cómputo, pero muchas veces buscan información financiera que les permita hacerse de algunos recursos. Si se hubiera instalado en una infraestructura sensible, donde la información que se almacena es de carácter confidencial o sensible, pues es explotable para estos grupos hacktivistas o para los que desarrollan estos malware.

¿Los sistemas informáticos del gobierno y de las instalaciones estratégicas están blindados?

-No hay nada que sea 100% seguro, esa es una máxima, lo cierto es que el gobierno federal ha venido trabajando, desde hace algunos años, en cómo proteger todo el ciberespacio mexicano. El año pasado se presentó la estrategia nacional de ciberseguridad, un parteaguas.

¿La UICOT protege la red informática del gobierno federal?

-Hoy, diferentes dependencias están participando para garantizar un internet seguro en nuestro país. Es importante señalar que no existe una barrera física para aislar el internet mexicano del mundial, al estar interconectados con todos los países, todos los riesgos que ocurran alrededor del mundo son riesgos que, eventualmente, podemos recibir en nuestro país, pero el siempre estar emitiendo boletines de cuáles son los mejores mecanismos de prevención, ayuda y, en caso de que no podamos prevenir, tener los protocolos de reacción para mitigar aquellos riesgos que se estén explotando y que una vulnerabilidad, haya sido explotada y que no tengamos una afectación.

Últimamente se ha mencionado una posible intromisión del exterior en el proceso electoral. ¿Ustedes podrían brindar apoyo técnico al INE para blindar su sistema y evitar que el instituto sea víctima de un ataque cibernético?

-Por supuesto que sí. Una de las líneas de acción de esta unidad es la protección de información y buscar la ciberseguridad de las diferentes dependencias, organismos y empresas.

Si el Instituto Nacional Electoral nos requiere para buscar proteger alguna de sus infraestructuras, por supuesto que lo haríamos.

Nosotros hacemos diferentes cosas, una de ellas es estar monitoreando la red pública de internet a través de lo que nosotros estamos buscando, que es la comisión de delitos en internet, como la venta de droga, de armas, de artículos sin tener los derechos de autor.

¿Cuentan con la tecnología necesaria para apoyar al INE?

-Eso dependería de qué es en lo que ellos quieren que los apoyemos, la infraestructura tecnológica del INE es amplia y tienen un área de ciberseguridad que ha venido trabajando de manera adecuada a lo largo de los años. Tienen un Comité de Ciberseguridad que les permite tomar medidas para mantenerse libres de los ataques cibernéticos, pero si en algún momento requieren apoyo, ahí estaremos.

¿Han detectado riesgos de ataques cibernéticos?

-Hemos estado trabajando de manera coordinada con diferentes agencias alrededor del mundo. Recientemente tuvimos un operativo con Interpol, de hecho continúa, en el que nos están dando información sobre algunos posibles ataques en contra de la infraestructura de nuestro país.

Nosotros validamos que realmente está ocurriendo esa situación, levantar un protocolo para poder mitigar ese riesgo y poner en operación la plataforma que haya sido afectada.

La UICOT es de reciente creación y tenemos que ir avanzando a un nivel de maduración tal, que nos permita tener un grado de operación óptimo para poder brindar todas las capacidades que requiere el ciudadano en materia de prevención y persecución de los delitos cibernéticos.

¿Se han visto vulneradas las instalaciones estratégicas del país?

No tenemos ningún caso documentado, como país, donde alguna instalación o alguna infraestructura crítica haya sido afectada de manera grave, no tenemos ningún caso en el país afortunadamente.

Creo que los protocolos que se han implementado para prevención y afectación de infraestructuras sensibles han funcionado adecuadamente, pero hay que estar reinventando estos protocolos, porque las actividades criminales evolucionan. (consultado en http://www.eluniversal.com.mx/elecciones-2018/pgr-se-previene-ante-hackers-electorales el 17 de enero de 2018, 21:31hs.).

20 **España se arma ante ataques cibernéticos.** Siguiendo el camino de la Unión Europea, el país está preparando una reserva de expertos contra amenazas o posibles injerencias, en medio de las versiones de presunta propaganda rusa proindependentista en Cataluña

Un periodista lee en Estambul un artículo sobre el ciberataque global con el virus Wannacry lanzado en mayo de

Jerónimo Andreu / Corresponsal. Madrid. Los ataques informáticos preocupan cada vez más a los gobiernos europeos. La creación de ciberreservas de expertos capaces de combatirlos, como la que este año planea lanzar España, es una prueba de ello.

El ataque a 141 mil ordenadores de todo el mundo por parte del virus extorsionador Wannacry en primavera de 2017 animó al gobierno español a acelerar una ley, aún en tramitación, destinada a crear una ciberreserva con 2 mil expertos en seguridad informática que trabajarían en situaciones de crisis bajo un Mando Conjunto de Ciberdefensa (MCCD).

El 3% de las agresiones contra sistemas públicos y empresas estratégicas españoles fueron de máxima gravedad, según el gubernamental Centro Criptológico Nacional. El equipo de ciberreservistas debería apoyar al ejército y los servicios secretos cuando se detecten amenazas de este tipo. Los candidatos que se buscan para el cuerpo son de perfiles distintos, principalmente informáticos, pero también periodistas para combatir las fake news, juristas que conozcan los límites legales de las intervenciones, sicólogos...

El proyecto se basa en experiencias similares en Holanda, Reino Unido, Estados Unidos e Israel. Los detalles por cerrar son muchos, como la remuneración de los reservistas, y reputados hackers españoles como Simón Roses o Ramón Pinagua han acusado al gobierno de “propaganda” por un proyecto con buenas intenciones pero sin definir.

IX. FUENTES DE CONSULTA

ABOSO, Gutavo Eduardo, *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación.* Ed. B de f. Buenos Aires, 2017.

ANTOLISEI, *Manuale di Diritto penale, Parte Generale,* Giuffré, Milano, 1947.

DONNA, Edgar Alberto, *La autoría y la participación criminal*, Granada, Comares, 2008.

FRANCO GUZMÁN, Ricardo, *el concurso de personas en el delito*, PGR, México, 1959, pp. 13-14.

HURTADO POZO, José, *Nociones básicas de Derecho penal de Guatemala, Parte General,* spi, Guatemala, 2000.

MAGGIORE, G., *Derecho Penal,* Temis, Bogotá, 1954.

RUIZ ANTÓN, Luis Felipe, *El fundamento material de la pena en la participación*. Madrid 1990. p. 51 (citado en Tesis Doctoral que presenta el Doctorando D. Carlos Daza Gómez, para la colación del Grado de Doctor en Derecho por la Universidad de Sevilla, 2014).

SOLER (*Derecho Penal Argentino,* Buenos Aires, 1956, T. II.

VON LISZT, *Tratado de Derecho Penal,* Reus, Madrid, 1929.

WELZEL, Hans, *Derecho Penal Alemán. Parte General*, Chile, 1987.

07.mar.2016 CSA, David Saúl Vela, 09.01.2017 Última actualización 10.01.2017 http://www.elfinanciero.com.mx/nacional/admite-el-lider-de-cibersecta-que-le-pagaron-por-crear-psicosis.html#.WHTucY8cbRE.twitter

México / Veracruz 6 ENE 2017 - 10:16 CST http://internacional.elpais.com/internacional/2017/01/06/actualidad/1483689835_154959.html

http://www.eluniversal.com.mx/elecciones-2018/pgr-se-previene-ante-hackers-electorales

https://www.seguridad.unam.mx/troyano-bancario-copia-propagacion-de-wannacry

http://www.eluniversal.com.mx/mundo/espana-se-arma-ante-ataques-ciberneticos

Un importante empuje publicitario a la iniciativa lo ha dado la crisis independentista en Cataluña, que ha suscitado nerviosismo en políticos y medios de comunicación por las sospechas de injerencias desde Rusia. Tras el referéndum independentista del pasado 1 de octubre, se han multiplicado los estudios que acreditan que cuentas en redes sociales activadas desde Rusia rebotaban propaganda favorable al secesionismo. Algunos medios se han apresurado a señalar al Kremlin como instigador de estas maniobras, pensadas para desestabilizar a la Unión Europea (UE).

En un encuentro con periodistas esta semana, el ministro de Exteriores español, Alfonso Dastis, aseguraba que era necesario diferenciar el hecho de que la propaganda se realizase desde Rusia (por empresas privadas contratadas para ello) y que el gobierno ruso fuera su responsable. Dastis explicó que esta confusión había causado tensiones entre Madrid y Moscú que ya estaban resueltas, pero insistió en que, independientemente del autor, los ataques preocupaban a España. A preguntas de EL UNIVERSAL, sin embargo, reconoció que la única prueba que tenía el gobierno de que hackers internacionales hubieran ayudado a difundir fake news sobre Cataluña era lo que publicaban los medios de comunicación.

El contrarrelato, la contrainfluencia y la contrarreputación se apuntan como algunas prioridades de la ciberreserva que organiza España. La UE ya aporta oficialmente un millón de euros anual a su grupo East Stratcom, dedicado a desmentir la propaganda contra las políticas de Bruselas, especialmente la que llega a los países de Europa del Este desde Rusia. Este grupo se creó en 2015 durante la guerra de Ucrania y su visibilidad ha aumentado a medida que líderes como la británica Theresa May han acusado a Moscú de intentar influir en su política nacional favoreciendo la distribución de informaciones falsas.

Las acciones mediante las que la UE teme que los hackers se involucren en sus procesos políticos van desde contratar publicidad en buscadores y redes sociales a activar bots que difundan falsedades, atacar a servidores, o alterar padrones electorales. En México el Instituto Nacional Electoral (INE) también reconoció recientemente a este diarioque registró intentos de agresiones cibernéticas desde el extranjero. De igual forma que en Estados Unidos se investiga si hackers rusos accedieron a los correos electrónicos de los candidatos en las campañas de 2016, México está alerta para que no ocurra lo mismo en las elecciones de 2018. (consultado en http://www.eluniversal.com.mx/mundo/espana-se-arma-ante-ataques-ciberneticos el 24 de enero de 2018).