Hacktivismo y Ataques DDoS: ¿Herramientas de Protesta Social o Delitos Informáticos?

La delgada frontera entre la desobediencia civil electrónica y la ciberdelincuencia.

Por **Joel A. Gómez Treviño[1]**

Este artículo pretende ser apto para abogados, informáticos e ingenieros. Escribir sobre *hacktivismo* amerita un análisis desde diferentes perspectivas, que he decidido agrupar en tres entornos: técnico, sociopolítico y jurídico. Dentro del entorno técnico abordaremos desde luego el tema de seguridad informática.

Si eres abogado ten paciencia, la primera parte puede parecerte poco interesante pero considero indispensable que los "no informáticos" comprendan la parte técnica para luego conocer los motivos detrás de estos ataques y finalmente sus consecuencias jurídicas.

ENTORNO TÉCNICO: ¿QUÉ ES? ¿CÓMO SE HACE? ¿ES PELIGROSO?

Para los que son ajenos al mundo del cómputo forense y la seguridad informática, vale la pena comenzar con algunas definiciones que ayuden al lector a comprender la metodología detrás de estos ataques y su impacto real en la sociedad de la información.

¿Qué es un DoS / DDoS? 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:

- 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.

[1] Abogado egresado del ITESM Campus Monterrey en 1995, con Maestría en Derecho Comercial Internacional por la Universidad de Arizona (Estados Unidos) y estudios de Posgrado en Liderazgo de Negocios y Derecho de Propiedad Intelectual Internacional realizados en Reino Unido. Cuenta con certificaciones en Aspectos Regulatorios del Gobierno Electrónico y Aspectos Legales del Comercio Electrónico de la Organización de Estados Americanos (OEA) y la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD). Ha impartido más de 150 conferencias en programas académicos y profesionales de México, Estados Unidos, Canadá, Costa Rica, Colombia, Ecuador, Italia y Asia.

- 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 tal vez miles de personas para que cada una de ellas desde sus respectivas trincheras (computadoras) inicie el ataque simultáneamente contra un solo objetivo. Este es parte del concepto de "hacktivismo" que veremos en la siguiente entrega de este artículo.

El DoS es un ataque "uno contra uno" y el DDoS es un ataque de "muchos contra uno". En términos no tan técnicos, 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 vuelve incapaz de responderlas. De ahí el nombre "denegación de servicios".

Imagine usted una línea telefónica de servicio al cliente (*call center*) que está preparada para recibir y atender a 100 llamadas diarias. ¿Qué pasaría si en lugar de 100 llamadas esa línea recibiera 100,000 llamadas telefónicas? Un fenómeno similar ocurre cuando estamos en un estadio presenciando un concierto masivo o cuando hay un terremoto o emergencia similar; todo el mundo quiere llamar al mismo tiempo, por lo que las líneas de celular simplemente se colapsan, impidiendo el servicio a los usuarios. Lo mismo sucede cuando un sitio web es embestido con un ataque DoS o DDoS.

<u>¿Es un solo tipo de ataque?</u> No, en realidad 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, (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).

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.

¿Qué NO es un DoS / DDoS? 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.

Diversos especialistas en seguridad informática y cómputo forense fueron entrevistados para la elaboración de este artículo, los cuales nos comparten su opinión sobre los siguientes cuestionamientos.

¿Qué tan sencillo es realizar un ataque DoS / DDoS?

Jorge A. Arciga, CIO de la Presidencia de la República.	Lamentablemente resulta ser extremadamente sencillo, dado que estos ataques se sustentan en ingeniería social. Los organizadores son similares a quienes organizan marchas y así mismo se reconocen. Aprovechan el desconocimiento de sus seguidores y de los mismos curiosos para incrementar el potencial de un ataque.
Adolfo Grego, Director de Tecnología de Mycros Electrónica.	Un ataque de negación de servicio puede ser tan simple o complejo como el atacante quiera. Puede requerir la participación de personas o ser completamente automatizado.
Alberto Ramírez Ayón, Gerente de Riesgo Tecnológico de una institución financiera internacional.	Hoy en día es relativamente fácil, descargando alguna herramienta como LOIC, definiendo el target u objetivo y que nuestra máquina comience a 'disparar' paquetes y lograr un ataque de DoS. En realidad no considero que se requiera un grado avanzado de habilidades, sino sólo un poco de curiosidad y tal vez, la 'voluntad' de querer ser parte de un movimiento (anti)social.
Rhett Nieto, ex Director de Sistemas del Ayuntamiento de Veracruz.	Ahora ya no es nada complicado realizarlo. Actualmente grupos como Anonymous han simplificado los ataques mediante webhives o scripts que corren desde páginas web, lo cual te agrega un nivel de discreción. También han liberado herramientas simples para realizar este tipo de ataques de una forma más fácil.
Andrés Velázquez, Presidente y Director	No es la dificultad de ejecutarlo, sino de tener las herramientas y la infraestructura para realizarlo. Un *script kiddie* bien

de Investigaciones Digitales de Mattica.	conectado (contactos) podría tener acceso a una plataforma automatizada que lo pudiera ejecutar. Ejemplo Zeus.

Como podemos apreciar, prácticamente todos los entrevistados coincidieron en un punto: es bastante sencillo ejecutar un ataque DoS / DDoS, contando con las herramientas (*scripts*) adecuadas. Desde hace más de una década, reconocidos expertos internacionales han emitido opiniones similares.

En febrero del 2000, Yahoo.com, eBay.com, CNN, ZDnet.com y Amazon.com, entre otros, fueron víctimas de un ataque masivo de denegación de servicios. Ante esta ola de agresiones, una conocida publicación de hackers llamada "*2600: The Hacker Quarterly*" publicó lo siguiente: *Sentimos pena por los sitios de comercio por Internet que se han sido víctimas de los ataques de denegación de servicio. Realmente lo sentimos. Pero no podemos permitir que ellos o alguien más a echen la culpa a los hackers. Dado que la capacidad de ejecutar un programa (que es todo lo que un DDoS es) no requiere ninguna habilidad de hackeo, alegar que los hackers están detrás de estos ataques indica algún tipo de conocimiento de los motivos y las personas involucradas*.

Winn Schwartau, autor de "CyberShock" e "Information Warfare", en relación a la herramienta conocida como "Flood Net" liberada por el grupo hacktivista EDT en 1999, afirmó entonces que "esto es un evento potencialmente perturbador que inclusive podría potenciar a hackers *aprieta-botones* y punks despistados con una actitud negativa".

Dentro de la amplia gama de delitos y/o ataques informáticos, ¿dónde ubican al DoS / DDoS en cuanto a peligrosidad e impacto?

Jorge Arciga comparte su visión desde la Presidencia: "Yo en lo particular, lo pondría en muy peligroso dado que podrían inhibir servicios a la comunidad que se encuentran publicados para respuesta inmediata. Un ejemplo sencillo es la declaración de impuestos que miles de contribuyentes hacen mensualmente; el encontrar inhibido un servicio de este tipo significaría una pérdida de ingresos tributarios, sanciones por incumplimiento, pero por sobre todo, un millonario costo a los contribuyentes que tendrían que regularizar su situación".

Adolfo Grego comenta que "Los ataques de negación de servicio para énfasis en medios son equivalentes a cerrar una calle o bloquear un edificio de gobierno: incomodan pero no son mortales. Me preocupa cuando estos ataques se usan como cortina de humo para esconder intrusiones que logran penetrar activos informáticos valiosos".

Alberto Ramírez, representando a la industria financiera opina que: "Dependerá del giro, ya que básicamente ataca la disponibilidad de un sistema o portal, por lo que si se ataca un sistema o portal que sólo es informativo o de poco interacción, el impacto podría no ser

grave; sin embargo si se ataca a un portal que realiza transacciones en línea, pues el impacto comienza a ser mucho muy crítico (bancos, ventas online, etc.) como los ataques a Visa, MasterCard y PayPal".

Rhett Nieto, como ex funcionario público y ahora desde la iniciativa privada afirma: "lo considero moderadamente peligroso porque por lo regular son ataques temporales, que solo buscan provocar una perdida en la continuidad del servicio".

Andrés Velázquez, desde la perspectiva de un investigador forense digital revela que "depende de la función del equipo que se ve afectado, por ejemplo: una empresa que realiza compra-venta y de eso depende su subsistencia el impacto es muy alto, a diferencia de una empresa que solo tiene un servidor para ofrecer sus servicios, la cual no genera un impacto económico a la organización. En cuanto a peligrosidad es bajo, ya que no es una intrusión, es simplemente el impedir el acceso".

De nueva cuenta los entrevistados convergen en una idea: "si el sitio web bajo ataque realiza transacciones financieras o comerciales, o brinda servicios informáticos, el impacto o daño puede ser muy grave".

Más detalles sobre el DoS los puedes encontrar en la página de Wikipedia.

ATAQUES CON MOTIVACIÓN POLÍTICA

Ahora veremos algunos conceptos para diferenciar el *hacktivismo* de otras actividades o conductas negativas en el ciberespacio, así como casos reales de ataques DDoS y hacktivismo en México, tanto históricos como del presente. Lo más importante, conoceremos qué son los *hacktivistas* y qué motivos persiguen.

LABERINTO CONCEPTUAL

Es común y desafortunado leer en la prensa el uso de términos no apropiados para describir hechos de violencia cibernética. El pasado 15 de septiembre la revista **Proceso** en su página web publicó una nota intitulada "*Tumba* Anonymous páginas web del gobierno". Este fue un hecho ampliamente divulgado en todo tipo de medios de prensa, tanto escrita como electrónica. No puedo afirmar que todos, pero si la mayoría de estos medios usaron las palabras "Anonymous *ataca* páginas del gobierno" en sus encabezados, en lugar de la suave frase "Anonymous *tumba* páginas del gobierno". El citado artículo inicia con una frase todavía más inapropiada (y de hecho falsa): "la red internacional de *ciberactivistas* Anonymous puso en marcha su Operación Independencia… con la que logró saturar y suspender sitios web de la Presidencia, la SEDENA y la SSP". Si bien el portal de la Presidencia fue objetivo del ataque DDoS, éste nunca fue "saturado y suspendido", como correctamente lo informaron otros medios y el mismo CIO de la Presidencia.

Para describir el mismo hecho, **Milenio** publicó "Anonymous *ataca* en México… páginas del gobierno de San Luis Potosí y Nayarit quedaron inhabilitadas por *hackers* de Anonymous", mientras que **CNN México** afirmó "el grupo de *piratas cibernéticos* Anonymous puso en marcha este jueves un *ataque* contra sitios web gubernamentales de México". Por su parte, **e-Consulta.com** tituló la nota "Atacan ciberactivistas portales de internet del gobierno federal".

Después de esta tormenta de términos, ¿quedará claro si "Anonymous" es un grupo de (1) hackers, (2) piratas cibernéticos o (3) ciberactivistas? ¿Las páginas de internet del gobierno fueron (1) atacadas, (2) tumbadas o (3) inhabilitadas? Aunque no existe un consenso universal sobre el significado de estos y otros términos, a continuación mencionaré lo que se entiende normalmente por cada uno de ellos.

Hacker es tal vez la palabra más difícil de definir, puesto que irónicamente tiene connotaciones tanto positivas como negativas. Para la prensa, los legisladores, las autoridades y la industria de las tecnologías de información (en otras palabras, para la mayoría de la gente), *hacker* es un ciberdelincuente que penetra ilícitamente servidores o sistemas informáticos, ya sea para borrar, copiar, conocer o modificar información sin autorización para hacerlo. También realizan otras acciones destinadas a inhabilitar o suspender el uso de sistemas informáticos. Para la comunidad *hacker*, este término se refiere a una persona experta en sistemas informáticos, que usualmente busca detectar fallas o huecos de seguridad en ellos sin fines "ilícitos". Ellos acuñaron el término **Cracker** para referirse al individuo que penetra sistemas o vulnera aplicaciones para violar medidas de seguridad o causar daños en ellos. La connotación negativa del término *hacker* es la que prevalece ampliamente en la comunidad legal y de seguridad informática.

Richard Power, en su libro *Tangled Web*, cita a la Dra. Dorothy Denning, profesora de la Universidad de Georgetown, en una importante conferencia ante el *World Affairs Council*, en diciembre de 1999 sobre Activismo, *Hacktivismo* y Ciberterrorismo. Ella clasifica este fenómeno de la siguiente manera:

- **(Ciber)Activismo** es el uso normal no disruptivo de Internet para apoyar una causa a agenda. Operaciones en esta área incluyen navegación en la web, construcción de sitios web y publicación de materiales en ellos, difundir publicaciones electrónicas y cartas por correo electrónico, y uso del internet para discutir asuntos, formar coaliciones y planear o coordinar actividades.
- ***Hacktivismo*** es el matrimonio entre el *hackeo* y el activismo; incluye procedimientos que usan técnicas de *hackeo* contra un sitio web con la intención de interrumpir las operaciones normales sin causar daños serios. Ejemplos son: protestas web y bloqueos virtuales, bombas automatizadas de correo electrónico, intrusiones a computadoras, y virus/gusanos informáticos.

- **Ciberterrorismo** es la convergencia del ciberespacio y el terrorismo. Incluye operaciones de *hackeo* políticamente motivadas con la intención de causar graves daños, como pérdida de vidas humanas o severos daños económicos.

Dicho lo anterior, es evidente que Anonymous NO es un grupo de activistas o ciberactivistas como erróneamente se refieren a ellos diversos medios de prensa. Sus actividades encajan perfectamente en la conducta de *hackers* y *hacktivistas*.

ENTORNO SOCIOPOLÍTICO: ¿QUIÉNES LO HACEN? ¿POR QUÉ LO HACEN?

Power en su libro *Tangled Web* nos ayuda a comprender el fenómeno de hacktivismo con esta frase: *Tal vez la imagen más romántica de un hacker es una tomada del viejo testamento: el joven David matando al gran tirano de Goliat con su honda. De hecho, muchos consideran al hacktivismo como una causa noble*.

¿Quién realiza este tipo de ataques (DDoS)? Tal vez para la mayoría la imagen de un *hacker* se nos viene a la mente rápidamente y casi de manera automática. Aunque suene raro, no siempre hay verdaderos *hackers* detrás de estos incidentes de seguridad informática. De hecho, la mayoría de las ocasiones quienes perpetran estos ataques son *hacktivistas* apoyados por gente común y *script kiddies*.

Aunque no lo menciona expresamente Denning en su definición, es claro que las actuaciones de los *hacktivistas* son la mayoría de las veces políticamente motivadas. Para muestra, los siguientes casos:

- Winn Schwartau es probablemente el único autor que tiene documentado el más viejo ataque DDoS "mexicano". En su libro "CyberShock" narra que en marzo de 1996, mexicanos promovieron "huelgas por internet" similares a las que habían ocurrido en Europa en 1995 y 1996 (ataques cibernéticos a sitios web franceses, italianos y estadounidenses, como protesta por sus políticas públicas). En mayo de 1996, hacktivistas lanzaron ataques de denegación de servicio al grupo de noticias de usernet llamado "alt.religion.scientology" en un intento aparente de sofocar la crítica e intolerancia de la Iglesia hacia sus detractores.

- Tanto Schwartau en "Cybershock" como Denning en su libro "Information Warfare and Security" documentan el tal vez más famoso ataque DDoS relacionado con México y hacktivistas. En septiembre de 1998, el grupo de hackers-hacktivistas llamado "*Electronic Disturbance Teather - EDT*", como muestra de apoyo y solidaridad a los Zapatistas Mexicanos, lanzó un ataque masivo de denegación de servicios en contra de sitios web del Pentágono, la Casa Blanca y del gobierno mexicano presidido en aquel entonces por Ernesto Zedillo.

Denning narra que en el año nuevo de 1994, insurgentes del EZLN ocuparon 6 pueblos en Chiapas. El ejército mexicano recuperó los territorios, pero los Zapatistas se esforzaron por compensar su falta de poder físico dominando el ciberespacio. Los Zapatistas y sus partidarios usaron internet para esparcir su voz sobre la situación en Chiapas y para coordinar sus actividades. Fue así como el EDT se enteró de esta problemática, y empezó a enviar anuncios a través de emails incitando a miles de personas a que se unieran en un acto de *Desobediencia Civil Electrónica* para detener la guerra en Chiapas. Brett Stalbaum, uno de los líderes de EDT, creó un programa de software llamado "*The Zapatista FloodNet*" para facilitar los ataques. Aunque no hay concordancia de la fecha exacta, pues Schwartau reporta que el ataque se llevó a cabo el 9 de septiembre de 1998 y Denning comenta que fue el 10 de abril del mismo año (o tal vez fueron dos ataques), lo cierto es que 18,615 personas en 46 distintos países, apoyaron desde sus computadoras el ataque masivo contra estos sitios de gobierno de México y Estados Unidos. Ricardo Domínguez, neoyorquino de padres mexicano, fue uno de los principales protagonistas del EDT y de este ataque DDoS.

El EDT planeaba repetir el ataque en contra del sitio web del Presidente Ernesto Zedillo, pero cambiaron de planes cuando un grupo activista de derechos humanos llamado "AME LA PAZ" protestó declarando lo siguiente: "*Nuestro grupo objeta cualquier tipo de ataque que viole la ley. Es claro que hay una guerra en Internet en la que los Zapatistas van ganando, pero la guerra real ha sido ganada dentro de las fronteras de la ley. El EZLN no sugiere ni desea que la sociedad civil que los apoya se involucre en acciones ilegales*." Lo interesante de esto es que, a pesar de que en esa época en México los ataques de DDoS no estaban contemplados en la ley como delitos, la conciencia de este grupo de derechos humanos y del EZLN era clara: cualquier ataque DoS / DDoS es (o debiera ser) ilegal.

Digno de llamar la atención es que, de acuerdo a una nota de la agencia periodística Reuters de Noviembre del año 2000, ***el término "hacktivismo" es atribuible a los Zapatistas***, refiriéndose a los ataques DDoS que en 1998 realizó el EDT como muestra de solidaridad al EZLN.

Dando un salto de casi tres lustros, podemos citar como los ataques hacktivistas (DDoS) más recientes en México los ocurridos recientemente, durante el mes de septiembre de 2011 en contra de diversos sitios web del gobierno federal y algunos gobiernos estatales.

- El 2 de septiembre Anonymous Iberoamerica lanzó un ataque de denegación de servicio (DDoS) contra las páginas web de la Cámara de Diputados, la Cámara de Senadores y de la Presidencia de la República, siendo exitosas las agresiones cibernéticas. Anonymous justificó sus acciones al señalar que la #opSegMex era una protesta contra las autoridades mexicanas debido al clima de violencia que

vive el país. Aunque el gobierno lo negó, estos ataques también resultaron en robo de información de diversas dependencias.

- Después de un mes de haber advertido el ataque, como un símbolo de protesta por la manera en la que gobiernan el país, el 15 de septiembre Anonymous lanzó la #OpIndependencia contra distintos portales del gobierno mexicano. Sergio López en bSecure reportó que esta "operación" significó ataques de negación de servicio (DDoS), robos de información y (web) *defacements*. La primera página web "tirada" fue la de la Secretaría de la Defensa Nacional, seguida por las del Congreso de Nayarit, la Secretaría (Federal) de Seguridad Pública, la Secretaría de Gobernación y el CISEN. La página de la Presidencia también fue severamente atacada, pero en esta ocasión no pudieron "tumbarla".

- El 26 de septiembre www.el5antuario.org publicó que "El grupo de ciberactivistas (sic) Anonymous México logró hoy "tirar" por unos minutos el portal del gobierno de Veracruz, en protesta por presuntas acciones emprendidas por la administración de Javier Duarte contra la libertad de expresión". Parte del comunicado que este grupo de *hacktivistas* publicó ese día dice:

  "*Estamos viviendo una de las medidas más autoritarias que ha tomado el gobierno Veracruzano en contra de su pueblo al aprobar la ley "antirumores", con ello coartando nuestra libertad de expresión y por lo tanto atentando a nuestras garantías individuales. En ésta nueva ley, todo aquel que supuestamente atente contra el orden público se convierte en "terrorista", perdiendo así su libertad física por los años que al sistema judicial se le antoje. […] Los "Twiteros terroristas" solo fueron víctimas de un gobierno nefasto que niega los hechos y a falta de información real, buscamos nosotros conocer la verdad. […] Anonymous México no va a descansar hasta que cada uno de sus ciudadanos tenga el valor de alzar la voz en contra del que lo oprime, hasta que cada uno de ellos tenga la capacidad de decir ¡BASTA! a tanta arbitrariedad.*"

Habiendo analizado el entorno sociopolítico del *hacktivismo*, podemos concluir por ahora que es una actividad que se traduce normalmente en ataques cibernéticos ejecutados como una forma de protesta social en contra del gobierno, una corporación u organización civil o religiosa.

CONSECUENCIAS E IMPLICACIONES JURÍDICAS

Es probable que mucha gente piense que el DDoS no es tan malo como lo pintan, después de todo, ¿qué tanto puede pasar si el portal se queda fuera de servicio unas cuantas horas? En teoría, cuando el "agotamiento de servicios" termina, las cosas vuelven a la normalidad. Particularmente en la comunidad *hacker* existe la creencia de que el

hacktivismo es solamente una manera justificada de expresar su descontento con determinada situación política, económica o religiosa, hecho que está protegido bajo la garantía de "libertad de expresión", y por ende, no hay nada ilícito en lo que hacen. ¿Qué tan cierto será esto?

ENTORNO JURÍDICO: ¿CUÁLES SON LOS DAÑOS? ¿ES UN DELITO? ¿CUÁLES SON LAS CONSECUENCIAS LEGALES?

¿Hay daños derivados de un ataque DDoS? ¿Cuáles son? Dependiendo de la intensidad y complejidad con la que se ejecuta un ataque DoS/DDoS, el agotamiento de servicios del sitio web que recibe la agresión puede durar minutos, horas o días en el peor de los casos.

Jorge Arciga, Alberto Ramírez y Andrés Velázquez coincidieron al ser entrevistados de manera independiente en un punto importante: si el sitio web bajo ataque DDoS presta servicios gubernamentales (por ejemplo, pago de impuestos o servicios), o realiza transacciones comerciales (como Amazon.com) o financieras (banca electrónica), el daño e impacto es muy grave, tanto para las empresas o instituciones dueñas de los portales como para los usuarios de los mismos.

Estimados de Forrester Research, IDC eXchange y Yankee Group predicen que el costo (daño) para un sitio web de una gran compañía de comercio electrónico que esté fuera de servicio 24 horas (víctima de un ataque DDoS) puede ser de $30 millones de dólares. En un caso real de una serie de ataques DDoS en contra de Amazon, Yahoo, y Bay y otros en el año 2000, Yankee Group estimó que las pérdidas acumuladas fueron de $1.2 billones de dólares.

Si el sitio web atacado no realiza transacciones financieras, comerciales o de gobierno, una interrupción en el servicio con frecuencia significa una pérdida económica importante, así como daño a la reputación del negocio o institución. El que un sitio web no esté disponible a los visitantes, representa además una pérdida de dinero que fue gastado en la creación del sitio web, hosting, publicidad y otras actividades dedicadas a la promoción del sitio web. Aún peor, los clientes actuales y potenciales buscarán otro portal donde hacer negocios. A esto faltaría agregar los costos involucrados en arreglar, reparar y/o actualizar servidores, software y bases de datos comprometidas.

Aún en el supuesto de que el sitio atacado no sea de una empresa, ni de gobierno, ni exista posibilidad alguna de lucrar con él (un blog, una página personal, etc.), la gente tiene derecho a leer, ver y/o disfrutar lo que ahí se encuentre. ¿Qué parte de "ataque" y "negación de servicios" pudiere considerarse legal, legítima o al menos justificada?

¿Puede considerarse un ataque de DoS / DDoS como *libertad de expresión*? Nuestro artículo 6° Constitucional establece que: "*La manifestación de las ideas no será objeto de*

ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito o perturbe el orden público."

La garantía individual consignada en el artículo 6° Constitucional, dice Ignacio Burgoa en su libro "Las Garantías Individuales", tutela la manifestación de las ideas. Puede haber dos formas de emitir o exteriorizar los pensamientos: la escrita o la verbal. ¿A cuál de estas dos se refiere el aludido precepto de nuestra Ley Fundamental? Burgoa concluye que el aludido precepto se contrae a la manifestación verbal u oral de las ideas (pensamientos, opiniones, etc.), la cual puede tener lugar en conversaciones, discursos, polémicas, conferencias y, en general, en cualquier medio de exposición por conducto de la palabra.

La libertad de publicar y escribir ("libertad de imprenta") está garantizada por el artículo 7° de nuestra Carta Magna: "*Es inviolable la libertad de escribir y publicar escritos sobre cualquier materia. […] La libertad de imprenta no tiene más límites que el respeto a la vida privada, a la moral y a la paz pública*."

Por lo tanto podemos concluir que de ninguna manera un ataque DoS / DDoS puede considerarse como un acto de "libertad de expresión" ni de "libertad de imprenta". Estas libertades no otorgan licencia para atacar bienes, propiedades o información de terceros.

¿Qué es un delito? Sin ánimo de profundizar en doctrina penal, diremos que un delito es definido como **una conducta**, acción u omisión que es: **típica** (contemplada en la ley), **antijurídica** (contraria a Derecho), **culpable** (hecho con dolo, culpa, negligencia o imprudencia) y **punible** (a la que corresponde una sanción o pena). Los actos u omisiones que reúnen estas características, son ejecutados con intención (culpa o negligencia) de dañar a otros. Cuando dichos actos u omisiones no se encuentran tipificados y sancionados por la ley penal, suelen considerarse como "actos ilícitos" o "delitos civiles".

Fernando Castellanos, en su libro "Lineamientos Elementales de Derecho Penal" nos dice que "la palabra delito deriva del verbo latino *delinquere*, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley. El artículo 7 de nuestro Código Penal Federal define al "delito" como el acto u omisión que sancionan las leyes penales.

¿Un Ataque de DDoS es delito? Antes de contestar conforme a Derecho Mexicano, es mi deber afirmar que en casi cualquier país con un grado avanzado de desarrollo tecnológico (que regularmente va de la mano con un buen desarrollo legislativo) un ataque DoS o DDoS está contemplado como delito. Veamos algunos breves ejemplos:

- **Convenio sobre la Ciberdelincuencia (Convenio de Budapest):** Este convenio nacido el 23 de noviembre del año 2001 en el seno del Consejo de Europa, en donde

hubo varios países ajenos a la Unión Europea que fueron miembros y observadores de este instrumento internacional. Los países que han firmado y ratificado el Convenio de Budapest son: Albania, Alemania, Armenia, Azerbaijan, Bosnia y Herzegovina, Bulgaria, Croacia, Chipre, Dinamarca, Eslovaquia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Islandia, Italia, Lativia, Lituania, Moldova, Montenegro, Noruega, Países Bajos (Holanda), Portugal, Romania, Serbia, Suiza, Macedonia, Ucrania, Reino Unido y Estados Unidos. Los países que solo lo han firmado pero está pendiente su ratificación son: Austria, Bélgica, Canadá, República Checa, Georgia, Irlanda, Japón, Liechtenstein, Luxemburgo, Malta, Polonia, Sudáfrica, Suecia y Turquía. Los miembros parte del Convenio pero que aún no lo firman ni ratifican son: Argentina, Australia, Chile, Costa Rica, Filipinas, México y República Dominicana. Es ley en los 32 países que ya firmaron y ratificaron este Convenio, lo siguiente:

Artículo 5 (1) – 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, alteración o supresión de datos informáticos.

- **España:** Como ejemplo de lo que los países que adoptaron (firmando y ratificando) el Convenio de Budapest en su legislación local tenemos a España. A partir del 23 de Diciembre de 2010 entrará en vigor la reforma del Código Penal está operada por la Ley Orgánica 5/2010, de 22 de junio, y establece el siguiente contenido para el artículo 264, apartados 1 y 2:

  1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años.

  2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años.

- **Estados Unidos:** El país que probablemente tiene la legislación más avanzada y extensa en materia de delitos informáticos es Estados Unidos. El Código de los Estados Unidos contempla en diversas secciones y artículos que pudieren tipificar el DoS / DDoS como delito:

18 U.S.C. § 1362. Líneas de comunicación, estaciones o sistemas. A quien voluntaria o maliciosamente interfiera de cualquier manera con la operación o uso de líneas o sistemas de radio, telégrafo, teléfono o cable, o voluntaria o maliciosamente obstruya, impida o retrase la transmisión de cualquier comunicación sobre dichas líneas o sistemas, o intente o conspire para hacerlo, deberá ser multado y/o sentenciado a no más de 10 años de prisión.

18 U.S.C. § 1030 (a) (5) (A) (i). A quien conscientemente provoque la transmisión de un programa, información, código o comandos, y como resultado de dicha conducta, intencionalmente cause daño sin autorización, a una computadora protegida, será sancionado con:

- *Multa y/o prisión por no más de 10 años.*
- *Multa y/o prisión por no más de 20 años en caso de reincidencia.*
- *Multa y/o prisión por no más de 20 años en caso de que derivado de la conducta descrita el delincuente conscientemente o negligentemente cause o intente causar lesiones corporales serias.*
- *Multa y/o prisión hasta por cadena perpetua en caso de que derivado de la conducta descrita el delincuente conscientemente o negligentemente cause o intente causar la muerte.*

"Computadora protegida" es definida por el artículo 18 U.S.C. § 1030 (e)(2)(b) como "una computadora que es usada en, o afecte el, comercio interestatal o internacional, incluyendo una computadora localizada fuera de los Estados Unidos que es usada en una manera que afecta una comunicación o el comercio interestatal o internacional." Como vemos, "computadora protegida" nada tiene que ver con seguridad informática o con mecanismos informáticos de protección para redes o computadoras.

"**Daño**" es definido por el artículo 18 U.S.C. § 1030 (e) (8) como "cualquier deterioro, insuficiencia o menoscabo a la integridad o disponibilidad de datos, programas, sistemas o información".

- **Colombia:** Fue tipificado como delito el DoS / DDoS en Colombia mediante una adición del artículo 1 de la Ley 1273 de 2009, publicada en el Diario Oficial No. 47.223 de 5 de enero de 2009:

Artículo 269 B: *Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.*

- **México:** A pesar de que existen los "delitos informáticos" en el Código Penal Federal mexicano desde el 17 de mayo de 1999, tristemente en su articulado no se contempla el ataque de denegación de servicios como delito. Urge que México firme y ratifique el Convenio de Budapest para estar a la altura de las circunstancias tecnológicas y el crimen cibernético que el mundo vive en la actualidad.

A lo largo de estas tres entregas que forman parte integral de este artículo, he hecho énfasis casi absoluto sobre el "ataque de denegación de servicios", pero debo reiterar que éste no es el único método, herramienta o ilícito realizado por los *hacktivistas* para promover sus fines o agenda política. Recordemos las palabras de la Dra. Denning, "*hacktivismo* es el matrimonio entre el *hackeo* y el activismo". Estos individuos realizan cualquier tipo de intrusión y vulneración informática a su alcance para lograr sus objetivos.

CONCLUSIONES

Federico Pacheco, gerente de Educación e Investigación de ESET Latinoamérica, dijo en entrevista para El Universal que "*si bien los inicios del hacktivismo se remontan a más de dos décadas, en estos últimos meses ha aumentado su repercusión a nivel mundial. Se trata de la utilización de herramientas digitales con fines ideológicos. En la mayoría de los casos, grupos hacktivistas organizados llaman al público a la participación por medio de redes sociales, para lo cual los proveen de las herramientas necesarias*". Informes de amenazas de McAfee del 2010 y 2011 confirman que "*los ataques de motivación política están en aumento en todo el mundo, concentrándose en destinos de redes sociales populares. […] Los hacktivistas, utilizaron Twitter, YouTube y Facebook para promover sus mensajes y eludir los medios de comunicación controlados por el gobierno*".

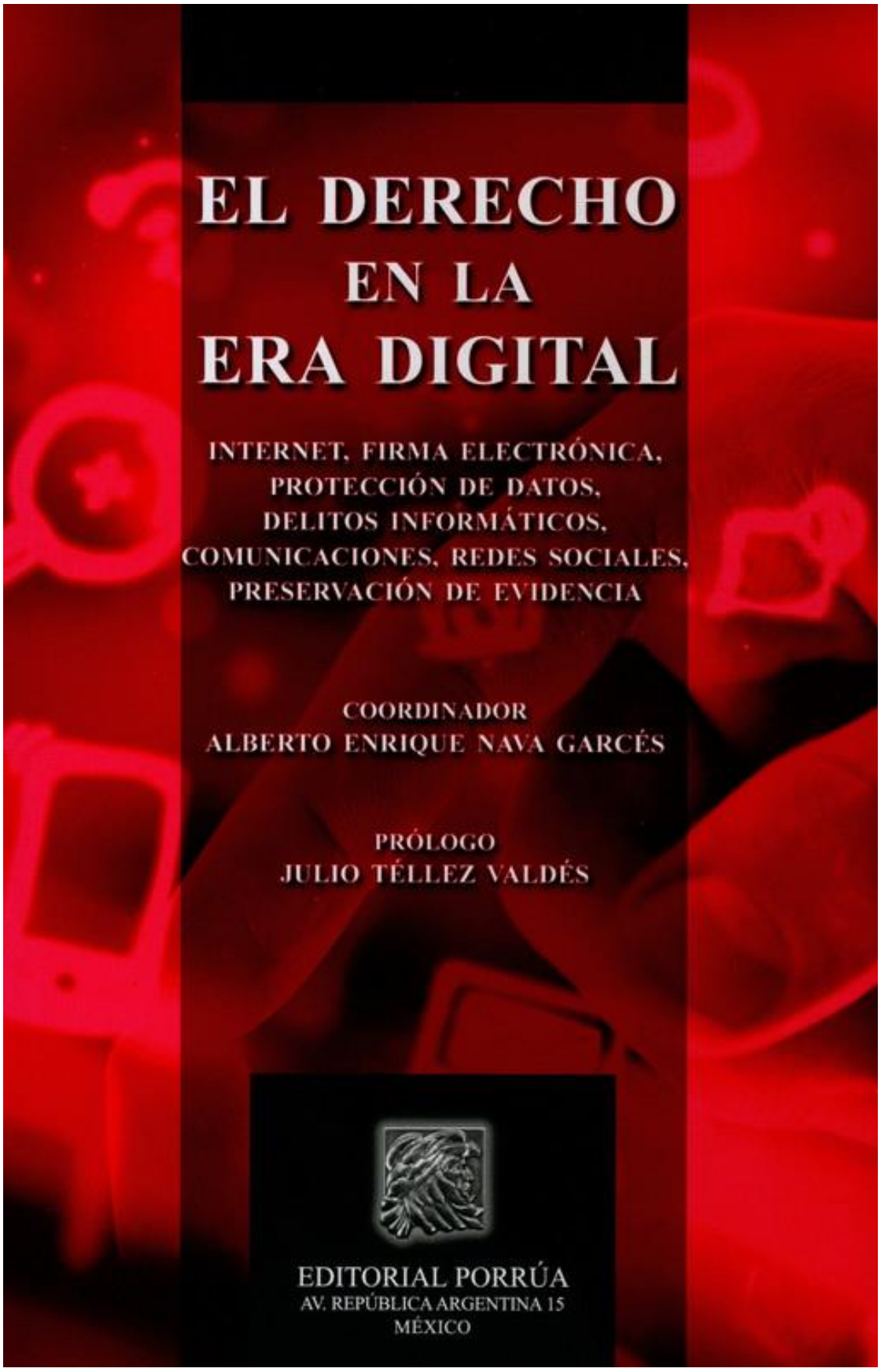
Winn Schwartau, en 1994 escribió para *Information Week*: "*La ciber-desobediencia civil (hacktivismo político) es oportuna, conmovedora, y potencialmente muy eficaz; es real y está al alcance de millones de personas. La gente ya no necesita tomar las calles. Quienes protestan con estas acciones necesitan la publicidad que les dan las noticias para enlistar más simpatizantes. Cuando se realizan ataques cibernéticos contra grandes organizaciones como la OTAN, lo importante no es afectar su capacidad de operar. Lo importante no es el hackeo en sí mismo, sino el efecto post CNN. Este tipo de ataques, aun siendo técnicamente menores, son una herramienta muy efectiva para hacerse publicidad*".

Tristemente las redes sociales y la prensa se han convertido en los principales aliados de los *hacktivistas*. Mientras las redes sociales son el medio idóneo para esparcir su ideología política, agenda y métodos de ataque, la prensa se convierte en el portavoz perfecto para decir: "aquí estamos, funcionamos coordinadamente, tenemos miles de seguidores en el mundo y nuestros ataques son exitosos… ¡únanse a nuestra causa!".

El *hacktivismo* está formado por dos componentes, uno positivo y otro negativo. Las matemáticas nos enseñan que restar un positivo o sumar un negativo es restar… así que nada bueno puede surgir de la mezcla de un componente positivo con un negativo. No

hay nada de malo en ser *ciberactivista*. Los medios de protesta pacífica y legítima son casi infinitos: creación de páginas web, blogs, foros, comunidades virtuales, promoción y campañas en redes sociales, envío de cartas de condena o desaprobación a través de correos electrónicos, etc. El problema inicia cuando a la legítima práctica de *ciberactivismo* se le suma el componente negativo del *hackeo*, considerado como delito virtualmente en todas partes del mundo. El resultado de este matrimonio es el *hacktivismo*, conducta a todas luces ilícita y nociva para la sociedad de la información.

Respondiendo a la pregunta que forma parte del título de este artículo, debo decir que si, el *hacktivismo* y los ataques DDoS son herramientas de protesta social, pero también deben considerarse como delitos informáticos. Ojalá México aprenda de los países de la Unión Europea, Estados Unidos y Colombia (entre otros), y pronto tipifique este fenómeno informático como delito en nuestro Código Penal Federal.


EL DERECHO
EN LA
ERA DIGITAL
INTERNET, FIRMA ELECTRÓNICA,
PROTECCIÓN DE DATOS,
DELITOS INFORMÁTICOS,
COMUNICACIONES, REDES SOCIALES,
PRESERVACIÓN DE EVIDENCIA
COORDINADOR
ALBERTO ENRIQUE NAVA GARCÉS
PRÓLOGO
JULIO TÉLLEZ VALDÉS
EDITORIAL PORRÚA
AV. REPÚBLICA ARGENTINA 15
MÉXICO