Revista de Bioética y Derecho
Perspectivas Bioéticas
www.bioeticayderecho.ub.edu - ISSN 1886-5887

DOSSIER SOBRE INTELIGENCIA ARTIFICIAL, ROBÓTICA E INTERNET DE LAS COSAS

Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas

Risks and vulnerabilities of the denial of service distributed on the internet of things

Riscos i vulnerabilitats de la denegació de servei distribuïts en internet de les coses

JAIRO MÁRQUEZ DÍAZ *

* Jairo Márquez Díaz. Licenciado en Matemáticas y Física. Doctor en Educación, Master en Bioética de la Universidad El Bosque. Nanotech Research & Develoment, Universidad de Cundinamarca, Colombia. E-mail: jemarquez@ucundinamarca.edu.co.

Resumen

La dependencia de la sociedad a la tecnología es cada vez mayor. En las ciudades el monitoreo se ha vuelto común, sea a través de sistemas de cámaras dispuestos por doquier, o a través de dispositivos y sensores que registran un sinnúmero de variables que literalmente miden el pulso de las mismas. En este artículo se expone el riesgo a nivel de la seguridad de la información sobre Internet de las Cosas (IoT), cuyo nivel de aplicación crece día a día y con ello, las vulnerabilidades en cuanto a conectividad y navegabilidad, debido a potenciales ataques de denegación de servicio distribuida (DoS). Bajo este mismo esquema, se presentan otros tipos de vulnerabilidades, relacionadas directa e indirectamente con el IoT y el DDoS, tales como el criptohackeo, el *blockchain*, las amenazas persistentes avanzadas (APT), el *ransomware* y la inteligencia artificial, exponiendo de manera general el riesgo potencial frente a la ciberseguridad en cuanto al uso y manipulación de la información.

Palabras clave: amenazas persistentes avanzadas; blockchain; criptohackeo; denegación de servicio distribuida; Internet de las cosas; inteligencia artificial; protocolos.

Abstract

The dependence of society on technology is growing, where the monitoring of cities has become common, either through camera systems arranged everywhere, to devices and sensors that record a number of variables that literally measure the pulse from the same. In this sense, this article exposes the risk at the level of security of information on the Internet of Things (IoT), whose level of application grows day by day and with it, vulnerabilities in terms of connectivity and navigability, due to potential distributed denial of service (DoS) attacks. Under this same scheme, other types of vulnerabilities directly and indirectly related to IoT and DoS are presented, such as cryptohack, *blockchain*, advanced persistent threats (APT), ransomware and artificial intelligence, generally explaining the potential risk in the face of cybersecurity regarding the use and manipulation of information.

Keywords: advanced persistent threats; artificial intelligence; blockchain; cryptohack; denial of distributed service; Internet of things; protocols.

Resum

La dependència de la societat a la tecnologia és cada vegada major. A les ciutats el monitoratge s'ha tornat comú, sigui a través de sistemes de càmeres disposats per onsevulla, o a través de dispositius i sensors que registren un sens fi de variables que literalment mesuren el pols d'aquestes. En aquest article s'exposa el risc a nivell de la seguretat de la informació sobre Internet de les Coses (IoT), el nivell de les quals d'aplicació creix dia a dia i amb això, les vulnerabilitats quant a connectivitat i navegabilitat, a causa de potencials atacs de denegació de servei distribuïda (DOS). Sota aquest mateix esquema, es presenten altres tipus de vulnerabilitats relacionades directa i indirectament amb el IoT i el DDoS, tals com el criptohackeo, el *blockchain*, les amenaces persistents avançades (APT), el *ransomware* i la intel·ligència artificial, exposant de manera general el risc potencial enfront de la ciberseguretat quant a l'ús i manipulació de la informació.

Paraules clau: amenaces persistents avançades; blockchain; criptohackeo; denegació de servei distribuïda; Internet de les coses; intel·ligència artificial; protocols.

1. Introducción

En la última década, la inteligencia artificial (IA) ha venido presentando un desarrollo sin precedentes, incorporándose rápidamente a diferentes campos científicos e industria en general, convirtiéndose en soporte de tecnologías emergentes como la minería de datos, la lingüística computacional, las tecnologías asistidas, la visión artificial, los videojuegos y mundos virtuales, entre otros. De igual manera, la IA se encuentra en campos como la medicina, la manufactura inteligente, logística, procesos industriales, sistemas de diagnóstico, educación, electrónica, agricultura, transporte, telecomunicaciones, finanzas, etc., mostrando con ello su gran diversificación.

Una particularidad de la IA, es que puede ser aplicada prácticamente en lo que se desee, cuya potencialidad se observa en desarrollos como la robótica, que se ha trasladado rápidamente a las tecnologías de la comunicación, transporte y dispositivos de control y monitoreo, empleados en hogares y edificios, que convergen al denominado Internet de las Cosas (IoT, *Internet of Things*).

Un aspecto fundamental de la automatización mediada por la inteligencia artificial en el IoT, es el nivel de seguridad; que es discutible, ya que en principio el código base del firmware o sistema operativo de cada dispositivo conectado o no a una red puede ser vulnerado, lo que es una falla de diseño y fabricación donde el factor seguridad fue subestimado. En este sentido, el *hackear* un sistema robótico permite sustraer datos de centros de investigación e industrias, e incluso puede causar accidentes o quitar vidas. No debemos olvidar que tanto los robots, cámaras, juguetes y electrodomésticos, entre otros dispositivos conectados a la web, pueden ser intervenidos mediante *malware* si no existe seguridad alguna en cuanto a su acceso. Normalmente los ciberataques a estos dispositivos se realizan mediante *botnets,* que se caracterizan porque permiten realizar ataques distribuidos de denegación de servicio (DDoS), que sobresaturan el tráfico de acceso a las páginas web con el fin de inhabilitarlas o tomar el control de los dispositivos.

El problema de los *botnets* como afirma Schneier (2017) es que se volverán más grandes y potentes sólo porque el número de dispositivos vulnerables aumentará de forma masiva durante los próximos años**.** Esta afirmación se sustenta en el hecho que permanentemente salen al mercado electrodomésticos y dispositivos electrónicos que son gestionados vía inalámbrica, cuya conectividad al ser permanente los hace más vulnerables a ataques continuos, donde la supervisión y/o configuración por parte del usuario es mínima.

2. Protocolos del IoT

El modelo de conectividad y navegabilidad de los dispositivos asociados al IoT se ajustan al modelo de protocolos TCP/IP. Sobre este modelo en particular se emplean diversos protocolos para la transferencia de datos según las características de los procesadores de los dispositivos IoT, que pueden ser de 8, 16, 32 y 64 bits. Con el protocolo IP (*Internet Protocol*) se garantiza la interoperabilidad entre los dispositivos IoT, en la que se manejan dos versiones IPv4 e IPv6; la primera solo funcionará hasta el 2020, mientras que desde esa fecha la segunda versión asumirá el 100% de las comunicaciones IP entre los diversos dispositivos alámbricos e inalámbricos conectados a internet.

Existen protocolos dedicados al IoT como el HTTP, REST, webSocket y XMPP, cuya operatividad puede estar sustentada en los protocolos TCP o UDP; y donde este último presenta ciertas limitaciones en cuanto a conectividad y funcionalidad, propios de su arquitectura. Un aspecto a mencionar frente a la seguridad del modelo TCP/IP, es que exhibe una serie de vulnerabilidades en cada capa que lo conforma (Aplicación, Transporte, Internet y Red), que pueden ser explotadas en cada protocolo asociado a las mismas. Por ejemplo, para el caso del IoT en la capa de red se presentan problemas de confidencialidad y de control de acceso; los cuales pueden ser vulnerados físicamente a través del *hardware* por el cual fluye la información. En la capa de red se pueden efectuar ataques que modifiquen o anulen un datagrama asociado a la IP del dispositivo objetivo, empleando técnicas de tipo *sniffing* y efectuar suplantaciones en el protocolo ARP o desactivación del filtro MAC, entre otros.

La capa de transporte tiene la función de transmitir datos vía TCP o UDP sobre datagramas IP. Aquí se presentan problemas de autenticación, integridad y confidencialidad, que son críticos para cualquier sistema de información por el que circulan datos sensibles. Algunos de los ataques más conocidos en esta capa es la denegación de servicio, que obstruye el flujo de datos inhabilitando la comunicación entre las partes. Otros tipos de ataques son el de tipo distribuido, *IP Flooding, snork, smurf, TCP/SYN flooding* y *teardrop*, *ping of death*, entre otros, cada uno con un grado de caracterización para sacar partido de las vulnerabilidades de diseño de esta capa. Finalmente, para la capa de internet, los ataques pueden ser a nivel de fragmentación, enmascarando los datagramas IP por otros que comprometen los datos que circulan entre diferentes puntos de una red.

Otros factores a tener en cuenta sobre la comunicación de IoT, es el uso de diferentes tecnologías como la NFC (*Near Field Communication*), RFID (*Radio Frequency Identification*) y WSN (*Wireless Sensor Networks*), donde cada una de ellas presenta sus propias vulnerabilidades (Santiago et al., 2018; Carrizo & Vargas, 2017; Sánchez et al., 2014). Cada una de estas tecnologías requiere de diversos protocolos, tales como:

1. Para la comunicación de sensores, actuadores y maquinaria, por ejemplo, robots industriales, PLC y SCADA. Los protocolos más utilizados son ModBus y ProfiBus.
2. Para sistemas domóticos se emplean los protocolos ModBus o KNX, que permiten la interconexión de sensores y actuadores.
3. Para grandes redes de pequeños dispositivos supervisados o controlados mediante un servidor *back-end*, se suele emplear el protocolo MQTT (Transporte de telemetría de cola de mensajes) que funciona bien sobre TCP o UDP (MQTT-SN). Otros protocolos relacionados son XMPP, CoAP y AMCIP.
4. Otros estándares de comunicación inalámbrica para sistemas domóticos es el ZigBee, el Zware, el IEEE 802.11 ah, Sigfox, LTE y LoRaWAN, entre otros.

Aparte de los protocolos estándar de comunicación como el Bluetooth, Ethernet o WiFi, existen otros relacionados con la capa de aplicación, que son diseñados por determinadas empresas para sus productos, tales como:

- MFI (*Made For Idevices*), cuyo propietario es Apple.
- Nest, su propietario es Google.
- Open Interconnect Consortium (OIC). Lo conforman Samsung, Intel, Dell, Atmel y Broadcom.
- The AllSeen Alliance. Los principales miembros son Haier, LG, Microsoft, Panasonic, Qualcomm, Sharp, Silicon Image, Technicolor y TP-Link.

En general, las empresas que trabajan con IoT, desarrollan sus propios protocolos adaptados a sus servicios, por lo que no hay una unificación universal que garantice la conectividad compatible entre dispositivos, abriendo una brecha a nivel de seguridad en este sentido.

3. Denegación de servicio distribuida e Internet de las Cosas

El Internet de las cosas o IoT, considerada como la cuarta revolución industrial (Schwab, 2016), está presente en la sociedad desde hace ya varios años. Se puede encontrar en electrodomésticos, teléfonos inteligentes, ropa inteligente, *wearables* (pulseras inteligentes, gafas de realidad aumentada, etc.), televisores inteligentes, videoconsolas, sistemas de transporte, edificios (cámaras de seguridad, climatización, controles de acceso, etc.), infraestructuras públicas (puentes, autopistas, parques, etc.), servicios públicos, componentes industriales, etc.

Una particularidad del IoT es la conexión entre dispositivos y el intercambio de información entre ellos, lo que plantea grandes desafíos en materia de seguridad. Como afirman Rose, Eldridge

& Chapin (2015) hay noticias sobre ataques a dispositivos conectados a Internet, donde el temor a la vigilancia y las preocupaciones relacionadas con la privacidad ya han captado la atención del público. La razón de esta afirmación subyace como afirma Barrio (2018) en que el IoT es una fuente de recolección de datos que crece exponencialmente y, en consecuencia, todo objeto pasa a ser un origen de información.

Un punto débil que aún no ha sido franqueado y que seguirá siendo un problema crítico para los próximos años en cuanto a la seguridad de la información, son los ataques por denegación de servicio distribuido (*Distributed Denial of Service*, DDoS), que inhabilitan la continuidad de comunicación corporativas con el exterior vía web, en la que se afecta no solo el ancho de banda, sino también la latencia y las tablas conmutadas de flujo de datos. Esto se logra debido a que se realizan múltiples peticiones a uno o varios servidores (web, correo electrónico, base de datos, proxy, etc.) desde diferentes lugares del mundo, con el objetivo de saturar el sistema hasta hacerlo colapsar, o efectuar ataques de fuerza bruta mediante *malware* especializados que escanean Internet en busca de dispositivos que estén conectados al IoT para obtener sus contraseñas, secuestrarlos y unirlos a una *bonet*[1].

En la actualidad, los mecanismos de defensa existentes presentan graves deficiencias, bien por la carencia de recursos y/o por la flexibilidad técnica y tecnológica que se dispone para hacer frente a ataques de tipo DDoS. Un riesgo potencial de las tecnologías emergentes como el IoT con respecto al DDoS, es precisamente el fallo de seguridad frente a la intrusión por terceros, donde la rápida expansión del IoT no solo en los ambientes del hogar, sino en las oficinas e industria, el entorno urbano y transporte, son un problema de seguridad mundial que crece.

¿Qué tan comprometedor puede ser un ataque de tipo DDoS? El objetivo de este tipo de ataque es interrumpir los servicios disponibles de conectividad vía Internet. Las motivaciones son diversas y variadas, desde resentimientos personales o corporativos, chantaje o extorsión, espionaje, competencia desleal, hasta razones políticas y/o militares. Un ejemplo relativamente reciente en el 2016, fue el ataque perpetrado a los sistemas de nombre de dominio o DNS (*Domain name Sytem*) de las empresas Twitter, PayPal, Spotify, Xbox, BBC y ESPNFantasySports, entre otras, que dejaron sin disponibilidad de acceso a los servicios a cientos de miles de usuarios en Estados Unidos durante varias horas, con nefastas pérdidas financieras por este concepto. Una razón del creciente flujo de

[1] Este es un *malware* que aprovecha las vulnerabilidades de los navegadores instalándose en computadores y/o servidores. La idea es que el virus infecte gran cantidad de sistemas formando las denominadas redes "*zombie*", aumentando con ellos la capacidad de procesamiento de ataques DDoS y Spam, entre otros, a objetivos específicos.

los ataques, es la disponibilidad de muchos factores, es decir, IoT débilmente seguros, mal configurados los dispositivos o portales de inicio. (The Associated Press, 2016)

El problema del DDoS no es nuevo, dado que para su ataque se emplean computadores y servidores mal configurados, conectándolos en redes Zombies. Lo innovador es el uso de diversos dispositivos asociados con el IoT para que actúen como puente de conexión y usarlos como armas digitales de ataque y/o espionaje, lo que en conjunto con las redes zombie estándar potencian el nivel de petición a los servidores objetivos del ataque, a miles o millones de veces lo usual. En este punto surge un verdadero problema: el IoT está en continuo crecimiento, Márquez (2018) afirma que para el 2020 existirán más de 50 mil millones de dispositivos conectados (omnipresentes) en las ciudades, es decir, más que la población mundial estimada para esta fecha (7.5 mil millones). Todos estos dispositivos estarán conectados a la red, por lo que se deduce una catástrofe si estos no están debidamente protegidos tanto en *software* (*Firmware*) como en *hardware*. Ejemplo de ello son los termostatos conectados a cámaras de seguridad y televisores inteligentes, los sensores de jardín, las puertas de garajes inteligentes, cubos de basura inteligentes, reguladores de luz, *wearables* para humanos y mascotas, equipos médicos, electrodomésticos, etc., todos estos sistemas se convierten en potenciales armas de espionaje y/o ataque.

Los dispositivos de la IoT se están implementado también en las grandes ciudades (*Smart Cities*), en edificios, en grandes y pequeñas infraestructuras en toda la ciudad con el objetivo de monitorear su estado, desde la supervisión de tráfico, control de semáforos, carreteras y puentes. Otro elemento más para sumar a esta compleja ecuación es lo relacionado a la seguridad metropolitana mediada por cámaras, robots y drones, que emplean conexión a dispositivos asociados al IoT, sobre todo sensores. Por consiguiente, si es hackeada esta infraestructura, la sociedad estaría a merced de los atacantes. Sobre este asunto se debe comentar, que no solo la delincuencia organizada y terroristas estarían tras este objetivo, sino gobiernos y milicias con el fin de monitorear a la sociedad a escala global de forma permanente, por ejemplo, la Agencia Nacional de Seguridad de los Estados Unidos.

Aunque existen diversas técnicas de mitigación para un ataque de tipo DDoS, son pocas las que han sido consideradas como viables a gran escala, debido a su eficiencia o complejidad a la hora de implementarse. Una propuesta reciente es tomar la infraestructura del *blockchain* y el *Smart Contracts*, que proporcionan la instrumentación requerida sin la necesidad de mantener el diseño y las complejidades de desarrollo de un protocolo tan nuevo (Rodríguez et al., 2017). Esta

propuesta se sustenta bajo la infraestructura de la nube cuyo grado de seguridad es alto, debido al filtrado de paquetes[2].

Una debilidad que se atribuye a la protección de la información es que está en manos del proveedor de servicios (DPS), lo que implica costos adicionales y una disminución en el rendimiento del servicio. Hay propuestas alternas que se están estudiando, como el uso de protocolos DOTS (DDoS *Open Threat Signaling*) (Rashidi & Fung, 2016), defensa colaborativa usando VNF (Funciones de red virtual), intercambio de eventos basado en FLow (FLEX), entre otros. Lo cierto es que sigue siendo un problema abierto cómo confrontar los ataques DDoS a gran escala, pues estos están creciendo tanto en el grado de sofisticación, duración y frecuencia, conforme el IoT lo hace, a lo que se suma la integración de la Inteligencia artificial (IA), aumentado la complejidad de seguridad en cuanto al flujo e integridad de los datos.

Otro asunto que relaciona el IoT, la IA y la ciberseguridad, son las fallas a nivel de *hardware*. Ejemplo de ello son los errores de diseño detectados en los *kerneles* o núcleos de los procesadores de Intel, AMD y ARM, denominadas como *Meltdown* y *Spectre* (CERT-MU, 2018; CERT-EU, 2018). Estos errores permitieron en su momento que *hackers* obtuvieran acceso a partes clave de los procesadores, instalando *malware* y robando claves de seguridad. (Giles, 2018) Aunque se desarrollaron parches de *software* y cambios de *hardware* para lidiar con este problema, siguen apareciendo nuevas variantes de fallas, lo que apunta que a futuro los problemas de *hardware* aumentarán, sumado a la incertidumbre de la transparencia por parte de los fabricantes. Las implicaciones son delicadas, debido a que la sociedad contemporánea es tan dependiente de la tecnología computacional, que hackear estos sistemas la compromete a estar a merced de los atacantes.

4. Criptohackeo

Es una nueva manera de *hackeo*, en la que se emplea *malware* que secuestra la capacidad de los sistemas de cómputo en la nube. Este tipo de ataque está más enfocado a grandes empresas y casas de cambio de criptomonedas. Esta es una nueva modalidad de robar dinero mejor que la del *ransomware*, que emplea como plataforma de ataque la potencia computacional de los dispositivos

[2] Dicho sistema consiste en un conjunto de dispositivos (*Firewalls* o cortafuegos) cuya configuración limita el paso y/o acceso de información en una red según ciertas reglas y protocolos. Por ejemplo, se registran los intentos de entrada y salida en una red, al igual que el acceso a internet o a determinadas aplicaciones, entre otras funciones.

móviles para minarlos con criptomonedas, que como es sabido, se premia bajo el supuesto que el dueño del dispositivo está realizando grandes transacciones bajo el modelo del *blockchain*.

El criptohackeo se asemeja parcialmente a un ataque de tipo DDoS, con la particularidad que no solo secuestran computadores, servidores y páginas web, sino dispositivos móviles inteligentes, que permite realizar transacciones fraudulentas a costa de la víctima, ganando mucho dinero en forma secreta. Ejemplo de *malware* con las características mencionadas son el *coinhive* y *cripto Miner* (Rüth et al., 2018), que fueron descubiertos en empresas importantes como Avira y Tesla.

Un problema que sigue en aumento es la comunicación asociada a las redes privadas y a la red oscura o *Darknet,* que es un 90% más grande que la comunicación estándar. Entre otros fines, esta red se emplea para cometer crímenes informáticos, compartir archivos comprometidos (personales, pornográficos, confidenciales, *software* ilegal, etc.) o para la compraventa de bienes y servicios prohibidos. (Arenas, 2018) Una propiedad esencial de la *Darknet* es que la comunicación es oculta, garantizando el anonimato e imposibilitando el análisis del tráfico de información; para ello se emplea una red diseñada para tal fin como el protocolo Tor.

Aunque los ataques informáticos se presenten al interior de la *Darknet*, el sistema es altamente flexible, dinámico y robusto como para adaptarse, minimizando los daños colaterales; característica de la que carece la Internet estándar. Ahora, cuando se emplea la *Darknet*, la probabilidad de hackeo con criptomonedas es alta, máxime cuando se opera bajo el modelo del *blockchain* y la contabilidad distribuida (Lipton & Sandy, 2018). Aunque este tipo de ataque es poco común en la actualidad, conforme sigan creciendo las operaciones con el *blockchain*, el nivel de riesgo también lo hará. Esto se debe a las particularidades técnicas y tecnológicas del *blockchain*, que facilita el intercambio de información entre grupos terroristas y delincuencia organizada, imposibilitando a las autoridades la intercepción de información sensible sobre atentados, narcotráfico, lavado de dinero y sicariato. Al combinar el *blockchain* con la Deep Web, la información legal o ilegal se torna casi imposible de rastrear (Hegadekatti, 2016; Bautista, 2015), debido a que este ciberespacio se considera literalmente como tierra de nadie, donde los datos fluye sin control alguno, dando pie a las operaciones de tipo DDoS.

5. *Ransomware*

Este tipo de ataque se caracteriza por encriptar los archivos de un computador o página web codificando la información, donde la víctima debe pagar por su rescate, que por lo general es mediante criptomonedas, razón por la cual hasta ahora no es posible de rastrear. Aunque no son

nuevos los ataques por *ransoware*, si lo es la forma de encriptar los archivos mediante algoritmos más sofisticados, que ocultan el rastro del atacante, la forma del pago y ataques a sistemas como la nube. En este sentido, lo que se espera en algunos años es que este tipo de ataque sea más destructivo y letal, ya que no solo los sistemas financieros, gubernamentales y militares estarán a su merced, sino que, al secuestrar sistemas vitales asociados con infraestructuras críticas de una ciudad o nación, se compromete la información y operatividad de todos los sistemas, paralizándolos, con la posibilidad de borrar y/o sustraer registros o modificarlos según lo que desee el atacante.

De lo mencionado anteriormente, se deduce que un ataque de tipo *ransomware* puede ser escalable siempre y cuando la infraestructura de las redes de comunicación lo permita, es decir, se facilita a través de la existencia de *software* y *hardware* vulnerables. Se debe tomar en consideración que, si un sistema permanece inactivo total o parcialmente, puede permitir acceso a información crítica mediante el uso de otros *malware* como los APT y dejar que éste realice las tareas para la cual fue programado, y luego, disponer de la información como mejor convenga. En este punto, el IoT no queda exento de sufrir un ataque de tipo *ransomware*, máxime si los dispositivos están siendo monitoreados por una página web o una aplicación móvil con un grado de seguridad efímero.

6. Inteligencia artificial y amenazas persistentes avanzadas

Aunque las publicaciones que argumentan ataques empleando ciber-armas basadas en IA sean escasos, no implica que no existan, puesto que lo que menos se quiere es que el público sepa de ello. Lo que sí se puede afirmar con certeza es que con la IA se pueden encontrar vulnerabilidades tanto en *software* como *hardware* de un sistema, pero ello requiere de equipos y recursos apropiados.

La inteligencia artificial (IA) jugará un papel fundamental a corto y mediano plazo en cuanto a la ciberseguridad. Actualmente, empresas de seguridad emplean modelos de aprendizaje automático combinados con redes neuronales y otras tecnologías relacionadas con la IA, con el fin de anticipar ataques a los sistemas informáticos e infraestructuras críticas, al igual que detectar *in situ* los que están ocurriendo en un sistema en particular. Desde esta perspectiva, no es utópico pensar aplicar ingeniería inversa para planificar ataques inteligentes propendidos por una IA, incluso contraatacar a otras IA. Por ejemplo, imaginemos el escenario de un ataque de este tipo a un vehículo inteligente, mediante el hackeo a la base de datos de la IA del vehículo, podría poner en peligro tanto a sus ocupantes como aquellas personas y vehículos a su alrededor.

Con la IA aplicada a ciberataques dirigidos contra las infraestructuras críticas, como sistemas de transporte, redes eléctricas, acueductos, oleoductos, hospitales, centros de suministros y

aeropuertos, entre otros, comprometen toda la seguridad y vida de las personas, bien de una ciudad como de toda una nación (Arnar, 2015). Este tipo de ataque se daría en varios frentes, empleando APT, *ransomware* y otros *malware* inteligentes, bien para secuestrar determinados sistemas críticos e inhabilitarlos temporalmente o destruirlos, con el fin de hacer colapsar su operatividad en el ciberespacio de los diferentes organismos gubernamentales de una nación.

La IA, tal como ha venido avanzando en los últimos años, puede amenazar la seguridad de cualquier país, bien por el uso malintencionado de grupos organizados al margen de la ley o por otros países. Una aproximación al respecto son las amenazas persistentes avanzadas (APT, *Advanced Persistent Threats*), que son un tipo de *malware* especializado diseñado a la medida para infectar dispositivos tanto a nivel de *software* como de *hardware*. Su objetivo es el robo, modificación, espionaje y sabotaje de información corporativa. Un APT posee rasgos de ataque de tipo furtivo (*stealth*), que combina técnicas de cifrado y algoritmos polimórficos muy relacionados con la IA. Márquez (2017) afirma que puede perdurar en el interior de un sistema informático por mucho tiempo sin ser detectado, aprovechando las vulnerabilidades propias de la infraestructura o de la misma arquitectura de los protocolos de comunicación en el empaquetado de datos en una red.

Un APT puede considerarse como un arma cibernética diseñada para ataques de objetivos específicos, en particular infraestructuras críticas, por lo que el IoT no es la excepción, ya que pueden ser interceptados e inhabilitar o destruir la comunicación entre dispositivos; esto se debe a que este tipo de *malware* puede filtrase a través de cualquier *software* o *hardware*, y desde allí empezar a escalar sistemas, por lo que el bloqueo con un ataque de tipo DDoS es factible. Aunque las APT son tan exclusivas y no abundan en internet, lo que se sabe de ellas es que sus gestores no son grupos delincuenciales organizados, sino específicamente gobiernos, que poseen los recursos técnicos y tecnológicos ilimitados para emprender este tipo de desarrollo y ataque dirigido. Ejemplo de ello, es la Agencia Nacional de Seguridad (NSA) de los Estados Unidos, señalada por diversos gobiernos de ser autora de espionaje electrónico avanzado y vigilancia global (Greenwald, 2014), cuyas acciones aparte de ser delictivas, vulneran de facto los derechos de privacidad.

La IoT cada vez incorpora más en sus desarrollos tecnológicos la IA, cuya conectividad vía internet y dispositivos móviles inteligentes denota un comportamiento exponencial, por lo que introducir un APT o *malware* similar a estos dispositivos aprovechando sus vulnerabilidades, puede realizarse bien cuando ya están en el mercado o desde su propia fabricación, tal como lo demostró Choi (2018). Esto implica escenarios plausibles como drones, robots y vehículos autónomos destinados a la cibercriminalidad de todo tipo. En cuanto a *software*, ya existen *bots* que suplantan a personas y *chatbots* que controlan emails mediante *malware* inteligente.

Como consideración final, controlar la IA de los dispositivos móviles y autos inteligentes está muy cercano, debido al desarrollo de redes neuronales que muestra errores de programación que pueden ser aprovechados para vulnerarlos, tal como lo demostró el sistema inteligente DeepXplore (Pei et al., 2017).

7. Discusión

En la industria del IoT se ha acuñado recientemente el término computación en el borde o *Edge Computig* (Shahzadi et al., 2017; Shi, et al., 2016), que Samaniego (2018) define como "la capacidad que el procesamiento de datos, las decisiones y el funcionamiento de los objetos, se produzca en el propio objeto y no en un servidor a cientos o miles de kilómetros de distancia".

¿Cuáles son las implicaciones de este nuevo desarrollo? Los dispositivos como cámaras digitales no solo captarán la imagen, además, mediante algoritmos basados en IA, la analizarán infiriendo aspectos relevantes de la misma, para luego subir esta información directamente a la nube. Lo mismo sucede con los sensores acoplados a los micrófonos, que captan el sonido de su entorno para analizarlo, discriminado ciertas frecuencias, filtrando aquellas que son relevantes para el estudio, subiéndolas a la nube.

Lo importante de las tecnologías mencionadas, es que la información se maneja en forma de cadena de bloques, es decir, emplea el *blockchain* como soporte de seguridad. Por consiguiente, la computación en el borde no trabaja sola aparte del IoT, sino que está íntimamente ligada a otras tecnologías como el *Mobile Cloud Computing* (Rehmani, 2017; Wang et al., 2015) y el *Collaborative Mobile Edge Computing* (Tran et al., 2017; Corcoran & Datta, 2016). Al ser tecnologías emergentes, el nivel de seguridad está en entredicho, comprometiendo la información de los usuarios si se criptohackea la nube.

Una variante del IoT está en el campo militar, denominado como Internet de las cosas en Batalla (*Internet of Battle Things, IoBT*). Esta tecnología está en permanente desarrollo, combinando complejas tecnologías de redes a gran escala con sistemas masivamente interconectados, donde Theron et al. (2018) afirman que la supervisión a nivel de seguridad cibernética por parte de los operadores humanos será cada vez más difícil, si no imposible. Este panorama deja un sinsabor sobre cuáles serán los sistemas que minimicen un riesgo potencial del *hackeo* de un sistema como el IoBT por parte de milicias extranjeras, grupos terroristas, delincuencia organizada, o por sistemas automáticos basados en IA.

La IoT presenta grandes beneficios y retos en materia de seguridad, donde la gran mayoría de dispositivos de consumo masivo para el hogar, oficinas y uso personal, incluyen aplicaciones para teléfonos inteligentes. Si esta tendencia se mantiene, el riesgo de recopilación de información personal por terceros es alto, máxime cuando los datos se trasmiten por redes no cifradas o por fallas de programación de las propias aplicaciones, a lo que se suma el descuido del propio usuario al no usar claves, o que éstas sean fáciles de descifrar.

Los ataques de DDoS combinados con las técnicas mencionadas, permiten ampliar su espectro de daño tanto a los sistemas de cómputo, como la IoT y dispositivos móviles, por la gran cantidad (y en aumento) de dispositivos interconectados en el mundo, por lo que emplear un ataque de tipo DDoS de día cero o basado en volumen es difícil de evitar: sólo se necesita una falla para que un *botnet* sature su objetivo, y ya está. Otros tipos de ataques más sofisticados, pero no menos comunes y altamente dañinos por el control que se adquiere a los sistemas, son los de protocolo, en este caso TCP dirigido específicamente a redes, *gateways*, servidores, *firewall* y equilibradores de carga.

8. Conclusiones

La sociedad muestra una tendencia a depender de la tecnología, donde el IoT está haciendo su parte, facilitando el acceso a información de diversos dispositivos *in situ*, sea que estén ubicados en el hogar, oficina, vehículos y la infraestructura de la ciudad, con el objetivo de mejorar la calidad de vida de las personas. Sin embargo, existe una preocupación por parte de los gobiernos y grupos relacionados con la ciberseguridad, debido a la fragilidad que presenta el IoT en cuanto a vulnerabilidad y riesgo en el tratamiento de la información. Esto se debe, en parte, a la proliferación de dispositivos relacionados con el IoT, que no cumplen determinados estándares de seguridad, exponiendo a la sociedad a ser atacada y espiada, lo que se suma a las vulnerabilidades propias de las arquitecturas de comunicación, aún por resolver.

Prevenir y proteger los ataques a las infraestructuras informáticas de cualquier organización son el fundamento de la ciberseguridad. Por consiguiente, las aplicaciones del IoT se extienden a entornos inteligentes, cuyo rango de acción se amplía rápidamente a redes de comunicación de próxima generación, exponiendo su visibilidad a las *Smart City*, *Green Systems* y *Transport Systems* para el análisis y visualización de datos en tiempo real. Con este tipo de aplicaciones y desarrollos en mente, se requiere de arquitecturas para IoT seguras e interactivas, compuestas por una infraestructura inteligente que permita modelar y simular el tráfico tomando las mejores decisiones. En este sentido, el desarrollo de la próxima generación de redes de sensores y diagnóstico remoto requerirán de una infraestructura de comunicación de alta

velocidad, ya en desarrollo, en la que se incorporan el reconocimiento de patrones, el análisis del comportamiento vehicular y estructural de edificaciones, puentes, vías, etc.

Se requiere de una unificación de protocolos de IoT y revisión del *software* y *hardware* de los dispositivos que han salido o saldrán al mercado, para minimizar el riesgo de vulnerabilidades que comprometan la información de los usuarios y sociedad en general, exponiéndolos a peligros que pueden ser prevenidos desde ahora.

Referencias

- AHMED, REHMANI E. (2016). *Mobile edge computing: opportunities, solutions, and challenges*. Future Generation Computer Systems. http://dx.doi.org/10.1016/j.future.2016.09.015
- ARENAS, ALEX. (2018). "La resiliencia de la red oscura. Un estudio logra describir las propiedades estructurales de la «Internet invisible» y explica por qué esta se muestra tan inmune a los ataques informáticos". *Rev. Investigación y Ciencia*, No. 498, pp. 12-14.
- ARNAR, JOSÉ. (2015). "Evolución de los modelos de confrontación en el ciberespacio". Documento de opinión, IEEE. es, pp. 1-25. http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO03-2015_Confrontacion_Ciberespacio_JL.Aznar.pdf
- BAUTISTA, DULCE L. (2015). "Deep web: aproximaciones a la ciber irresponsabilidad". *Revista Latinoamericana de Bioética* 15(1), Ed. 28, pp. 26-37.
- BARRIO, ANDRÉS M. (2018). *Internet de las cosas*, Madrid, Editorial REUS.
- CARRIZO, CINDY & VARGAS, MIGUEL. (2017). "Estándar, seguridad, vulnerabilidades y riesgos para la automatización del hogar". *Rev. de Iniciación Científica*, 3(1), pp. 1-6.
- CERT-EU, Computer Emergency Response Team. Security Advisory 2018-001. *Meltdown and Spectre Critical Vulnerabilities*. January 11, v1.1. http://cert.europa.eu/static/SecurityAdvisories/2018/CERT-EU-SA2018-001.pdf
- CERT-MU, Computer Emergency Response Team of Mauritius (2018). *Meltdown & Spectre vulnerabilities, National Computer Board. Whitepaper.* http://cert-mu.govmu.org/English/Documents/White%20Papers/MELTDOWN%20-%20CERTMU%20WHITEPAPER.pdf
- CHOI, CHARLES Q. (2018). "Lo siento, Dave". *Rev. Investigación y Ciencia*, No. 499, abril, p. 8.

- CORCORAN, DATTA SK. (2016). "Mobile-edge computing and the internet of things for consumers: extending cloud computing and services to the edge of the network". *IEEE Consum Electron Mag* 5(4), pp.73–74.
- GILES, MARTÍN. (2018). "Estos han sido los peores ciberataques en lo que llevamos de 2018". *MIT Technology Review*, Recuperado el 11 de marzo de 2019, en: https://www.technologyreview.es/s/10339/estos-han-sido-los-peores-ciberataques-en-lo-que-llevamos-de-2018
- GREENWALD, GLENN. (2014). *No place to hide. Edward Snowden, the NSA and the Surveillance State.* EE. UU. Hamish Hamilton.
- HEGADEKATTI, KARTIK. (2016). "Regulación de la Web profunda a través de Cadenas de Bloques Controladas y Redes de Cripto-Moneda". Recuperado el 10 de mayo de 2019, en: https://ssrn.com/abstract=2888744 o http://dx.doi.org/10.2139/ssrn.2888744
- JAN, RÜTH; TORSTEN, ZIMMERMANN; KONRAD, WOLSING & OLIVER HOHLFELD (2018). "Digging into Browser-based Crypto Mining". IMC '18, October 31–November 2, 2018, Boston, MA, USA, arXiv:1808.00811v2 [cs.CR]
- LIPTON, ALEXANDER & SANDY, PENTLAND. (2018). "Hacer saltar la banca". *Investigación y Ciencia*, No. 498, pp. 16-23.
- MARQUEZ, JAIRO E. (2017) "Armas cibernéticas. Malware Inteligente para ataques dirigidos" *Ingenierías USBMed*, 8(2), pp. 48-57. DOI 10.21500/20275846.2955
- MARQUEZ, JAIRO E. (2018). "Seguridad metropolitana mediante el uso coordinado de Drones" *Ingenierías USBMed*, 9(1), pp. 39-48.
- PEI, KEXIN; CAO, YINZHI; YANG, JUNFENG & JANA, SUMAN. (2017) "DeepXplore: Automated Whitebox Testing of Deep Learning Systems", *SOSP*, Shanghai, China arXiv:1705.06640v4 [cs.LG] 24 Sep 2017.
- RASHIDI, B., FUNG, C. "CoFence: a collaborative DDOS defence using network function virtualization". In: *12th International Conference on Network and Service Management* (CNSM 16), October 2016.
- RODRIGUEZ, BRUNO et al. (2017) Tuncer D. et al. (Eds.). "A *Blockchain*-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts. Security of Networks and Services in an All-Connected World". *11th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security*, AIMS, LNCS 10356, pp. 16–29. Zurich, Switzerland, July 10–13, Proceedings, Springer Open. DOI: 10.1007/978-3-319-60774-0 2

- ROSE, KAREN; ELDRIDGE, SCOTT & CHAPIN, LYMAN. (2015). *La internet de las cosas - Una breve reseña para entender mejor los problemas y desafíos de un mundo más conectado*, Internet Society (ISOC). Recuperado el 10 de mayo de 2019, en: https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf
- SAMANIEGO, JUAN F. (2018) "Ya es el año del Internet de las Cosas: estas son sus tendencias". Recuperado el 8 de enero de 2019, en: https://www.nobbot.com/redes/tendencias-en-el-internet-las-cosas/
- SÁNCHEZ, JOSÉ; LÓPEZ, LOURDES & MARTÍNEZ, JOSÉ. (2014) "Solución para garantizar la privacidad en internet de las cosas". *El profesional de la información*, 24(1), pp. 62-70. http://dx.doi.org/10.3145/epi.2015.ene.08
- SANTIAGO, ANDRÉS et al. (2018) "Modelo de Seguridad para Garantizar la Integridad de Pagos Móviles sobre Near Field Communication (NFC)". *Rev. Espacios*, 39(19), pp. 16-30.
- SCHNEIER, BRUCE. (2017) TR10: "Ejércitos de las cosas zombi". Recuperado el 9 de mayo de 2019, en: https://www.technologyreview.es/s/6823/tr10-ejercitos-de-las-cosas-zombi
- SCHWAB, KLAUS. (2016) *La cuarta revolución industrial*. Barcelona, Editorial Debate.
- SHAHZADI, SONIA; IQBAL, MUDDESAR; DAGIUKLAS, TASOS & UL, QAYYUM ZIA. (2017) "Multi-access edge computing: open issues, challenges and future perspectives", *Journal of Cloud Computing: Advances, Systems and Applications* 6(30), pp. 2-13, DOI 10.1186/s13677-017-0097-9
- SHI, FELLOW; CAO, JIE; ZHANG, QUAN; LI, YOUHUIZI & XU, LANYU. (2016) "Edge Computing: Vision and Challenges", *IEEE Internet of Things Journal*, 3(5), Doi 10.1109/JIOT.2016.2579198
- THE ASSOCIATED PRESS (2018). "Hackers Used 'Internet of Things' Devices to Cause Friday's Massive DDoS Cyberattack". Recuperado el 8 de mayo de 2019, en: http://www.cbc.ca/news/technology/hackers-ddos-attacks-1.3817392
- THERON, THALES P. et al. (2018) "Towards an Active, Autonomous and Intelligent Cyber Defense of Military Systems: the NATO AICA Reference Architecture". *International Conference on Military Communications and Information Systems*, Warsaw, Poland, 22nd - 23rd May 2018.
- TRAN, TX; HAJISAMI, A.; PANDEY, P. & POMPILI D. (2017). "Collaborative mobile edge computing in 5g networks: new paradigms, scenarios, and challenges". *IEEE Commun Mag* 55(4), pp. 54–61.
- WANG. X.; HAN, G., DU, X. & RODRIGUES, J. (2015) "Mobile cloud computing in 5g: emerging trends, issues, and challenges" [guest editorial]. IEEE Netw 29(2), pp. 4–5.

Fecha de recepción: 1 de diciembre de 2018

Fecha de aceptación: 12 de marzo de 2019