CIBERATAQUES A UN PASO DE LA CIBERGUERRA

*José Antonio Amaro López
**Citlalli Rosalba Rodríguez Rodríguez
***María del Carmen Macías Huerta
****María Dolores Andrade García

*Centro Universitario de Ciencias Sociales y Humanidades, Universidad de Guadalajara, Jalisco, México. Docencia y Tecnología.

**Universidad de Guadalajara, Jalisco, México. Docencia y Tecnología.

***Centro Universitario de Ciencias Sociales y Humanidades, Universidad de Guadalajara, Jalisco, México. Tecnología, Desarrollo Regional, Marginación y Estudios Urbanos

****Centro Universitario de Ciencias Sociales y Humanidades, Universidad de Guadalajara, Jalisco, México. Docencia, Tecnología y Geografía de la salud.

Articulo Recibido: 28 de agosto 2017. Aceptado: 16 de octubre 2017.

RESUMEN. El presente trabajo muestra los avances respecto a la regulación del ciberespacio y como los ciberataques han contribuido a esto debido al impacto económico y social. Es fundamental abordar los trabajos que la Organización de las Naciones Unidas (ONU) y el EastWest Institute (EWI) han realizado para regular el ciberespacio y prevenir una posible ciberguerra. Por tal motivo se realizó un análisis de caso donde se abordan trabajos sobre ciberataques y ciberseguridad en el ámbito internacional, tanto de agencias como de organismos que trabajan estos aspectos. Encontrando en este análisis que cada día se incrementan las incursiones por parte de terceros a la infraestructura cibernética de todos lo países, y que esto puede generar el inicio de las ciberguerras en un futuro cercano, por lo económico y lo rápido que resulta el realizar esta invasión virtual.

Palabras Clave: ciberconflicto, ciberespacio, regulación del ciberespacio.

INTRODUCCIÓN.

El presente trabajo muestra los avances respecto a la regulación del ciberespacio y como los ciberataques han contribuido a esto debido al impacto económico y social. Es fundamental abordar los trabajos que la Organización de las Naciones Unidas (ONU) y el EastWest Institute (EWI) han realizado para regular el ciberespacio y prevenir una posible ciberguerra. Por tal motivo se realizó un análisis de caso donde se abordan trabajos sobre ciberataques y ciberseguridad en el ámbito internacional,

tanto de agencias como de organismos que abordan estos temas.

DESARROLLO.

En la historia del ser humano ha estado presente el conflicto armado entre sus integrantes, ya sea por lograr el control de los recursos necesarios para sobrevivir (causas económicas), por cuestiones políticas-ideológicas o de índole religioso; como el caso del Imperio Romano cuyo interés era la expansión del territorio; o en el caso de la guerra en Siria que “tiene sus orígenes en la corrupción, en la captura política, en la pobreza, en la violación de derechos humanos y en la desigualdad” (San Pedro, 2015).

El conflicto armado va de la mano con una estrategia de combate, armamento y un campo de batalla en cual se desarrolla. Por ello, los ejércitos de cada país buscan tener un dominio militar en diferentes ámbitos de combate: el terrestre, el aéreo, el naval y, en vías de desarrollo, el espacial, incluyendo el ciberespacio.

El campo de batalla espacial emerge como tal, debido a que la sociedad moderna depende de las comunicaciones y de la conexión a Internet para desarrollar gran parte de sus actividades, y son los satélites espaciales los que proveen estos servicios; además, parte de la infraestructura crítica, de comunicación, transporte aéreo, comercio marítimo, servicios financieros, climatológicos y ambientales, también son soportadas por estos aparatos (Lewis y Livingstone, 2016a).

Si el espacio exterior es un lugar viable y no tan cercano para ser atacado, el ciberespacio resulta bastante atractivo y accesible para ser utilizado como campo de batalla, porque con una computadora, una conexión a Internet y conocimientos técnicos es posible acceder, robar y borrar información de otro equipo de cómputo. Así, es posible atacar la infraestructura crítica de los países, como las centrales nucleares, el sistema financiero, el sistema de transporte, entre otros.

La ciberguerra es definida por Rauscher y Yaschenko (2011: 30, traducción propia) como “un incremento o presencia de un ciberconflicto entre una o más naciones estado, en donde los ataques cibernéticos son realizados por otras naciones en contra de la infraestructura cibernética

como parte de una campaña militar". El campo de batalla es el ciberespacio, que definen como "un medio electrónico a través del cual la información es creada, transmitida, recibida, almacenada, procesada y borrada" (2011:20, traducción propia). Cabe señalar que este campo no es real, es creado por el hombre mediante el uso de dispositivos electrónicos, que al estar interconectados crean el ciberespacio.

Con estos dos conceptos es posible abordar otros importantes como el ciberconflicto, guerra cibernética, ciberinfraestructura, ciberinfraestructura crítica, (Rauscher & Yaschenko, 2011). entre otros, que al ser analizados definen aspectos virtuales y físicos que integran el ciberespacio, y por lo tanto, son susceptibles a ser atacados con la finalidad de causar algún daño físico, económico o informacional, que no permita a las personas tomadoras de decisiones, responder ante un ataque a su infraestructura considerada como crítica.

La estrategia que una persona, un grupo o país busca desarrollar al momento de realizar un ataque cibernético, de acuerdo con Miller y Kuehl (2009, traducción propia), es:

- Interrumpir las comunicaciones enemigas y las líneas de abastecimiento de suministros.
- Distraer y confundir al equipo de comando, así como disminuir el control que tiene el enemigo sobre las estrategias que ha de emplear para atacar.
- Afectar los movimientos de las fuerzas militares.
- Crear oportunidades para desarrollar un ataque estratégico sobre la infraestructura del enemigo.
- Debilitar y distraer la cohesión social y política, incluso antes de que se presente el conflicto.
- Moldear las percepciones globales acerca del conflicto.

Los mismos autores indican que podrían generarse nuevas estrategias militares, definidas como operaciones de información e infraestructura donde:

- Es posible combinar las estrategias anteriores, con otro tipo de operaciones, como las terrestres, navales o aéreas.
- Permitirían operaciones puntuales y limitadas dirigidas sobre puntos específicos de la infraestructura enemiga.
- Permitirían contar con metas estratégicas, operativas y tácticas.
- Ofrecen importantes estrategias asimétricas de combate, para ser utilizadas sobre la sociedad y los militares, dependientes de las capacidades de los sistemas en red.
- Proporcionan importantes ventajas al primer agresor, porque se combina con la relativa facilidad de iniciar un ataque mediante la aplicación de operaciones de información e infraestructura mediante Internet.
- Se limitan los ataques mediante el uso de estrategias de adaptación y desarrollo de capacidades de contraataque.
- Se limitan las acciones de contraataque debido a la dificultad inherente que tiene Internet de identificar al agresor.
- Se crea la necesidad de que otras fuerzas militares también desarrollen capacidades para realizar ciberataques, con la finalidad de defender su territorio (Miller y Kuehl, 2009, traducción propia).

Estas estrategias ya se han aplicado en el ciberespacio y es posible mencionar algunos ciberataques que, aunque no han llegado a escalar al nivel de provocar una ciberguerra, sí han dado la pauta para formular los puntos anteriores y buscar que los países identifiquen su ciberinfraestructura crítica, sus puntos débiles y los reparen, con el fin de no ser atacados.

El caso más impactante hasta el momento es el gusano Stuxnet, en junio de 2010, en Irán, donde se mostró la capacidad para controlar equipos de cómputo mediante un programa de 500 kilobytes, con el cual fue posible infectar 14 compañías, incluyendo una planta de uranio enriquecido. En esa ocasión el autor podría espiar las computadoras infectadas y, si lo deseaba,

operar los equipos industriales de estas empresas (Kushner, 2013).

El caso más reciente es el *WannaCry ransomware*, que infectó más de 200,000 computadoras en 150 países, el 12 de mayo de 2017, entre las cuales se encontraba equipo de cómputo de hospitales, fábricas, escuelas y tiendas. Este virus aprovechó encripta los datos del equipo infectado y dejar sin acceso al usuario, y para desencriptar la información, se solicitaba realizar un depósito a una cuenta que operaba mediante la moneda virtual conocida como *Bitcoin*.

Después de estos ataques, los militares comenzaron a hablar de la posibilidad de una ciberguerra (que hasta el momento no se ha presentado, o al menos no se conoce de alguna). Como los ciberataques dan cuenta de las posibilidades que existen de llevarse a cabo, las naciones Estado están capacitando a su personal militar y sus policías, en universidades especializas en el combate y defensa de su infraestructura que se encuentra en el ciberespacio.

Además de preparar a su personal para evitar los ciberataques (y una posible ciberguerra), en vista del incremento de estos y del daño que pueden causar, el EastWest Institute (EWI) ha estado trabajando desde 2009, en colaboración con expertos en tecnologías, expertos en derecho, con empresas privadas que desarrollan tecnología, con embajadores de distintos países, entre otras personas interesadas, sobre temas como la regulación del ciberespacio y el posible desarrollo de una ciberguerra.

Como parte de estos trabajos de regulación, en 2009 el EWI, en colaboración con la Sociedad de Internet China, realizó acuerdos para limitar el envío de correos spam,(ya que se tenía identificado que la mayoría de estos provenían de este país asiático y la difusión de este tipo de correos consume bastante el ancho de banda de Internet; además, es una estrategia para hacer uso del phishing, donde se envían correos con la finalidad de que el usuario descargue un archivo infectado o proporcione información privada para luego sea utilizada por los atacantes).

También en ese año se hizo hincapié en la amplitud y rapidez con que se han estado

llevando a cabo los ciberataques, y que representan una grave amenaza para las infraestructuras críticas, para el ejército y las finanzas en todo el mundo (Nagorski, 2010).

Para 2010 el EWI logró reunir a Rusia y Estados Unidos para colaborar en ciberseguridad y firmaron el documento titulado *Derechos y responsabilidades en el ciberespacio: Equilibrar la necesidad de seguridad y libertad* (2010), donde se expresa la necesidad de nuevas leyes internacionales que sustenten y proporcionen un marco legal para regular las actividades que se pueden llevar a cabo en Internet y cómo rastrear la fuente de un ciberataque. Además se identificó la necesidad de crear de manera consensuada un glosario de términos donde se establecieran conceptos sobre ciberseguridad, y que se pudieran utilizar para el mejor entendimiento entre las partes. Así, en 2011 se presentó el primer glosario de términos sobre ciberseguridad "*Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations*" (2011) y en 2014 se actualizó contando con alrededor de 60 definiciones.

Para 2012 el reporte anual del EWI (Stern, 2013) contabilizó 115,000 víctimas de ciberataques cada día, pérdidas mundiales (anuales) por 288 mil millones de dólares y surgió otro foco de atención, el desarrollo del *cloud computing* o cómputo en la nube.

Pero fue en 2013 cuando el EWI inició con los trabajos para comprender la importancia del riesgo de la seguridad, y se planteó una estrategia para generar estadísticas que permitan mostrar un panorama real de la situación y buscar soluciones que realmente ayuden a disminuir o anular el riesgo de estar conectados a la red.

Al igual que el EWI, la Organización de las Naciones Unidas (ONU) también ha buscado avanzar en el tema de la ciberseguridad desde el año 1998, cuando la federación Rusa presentó un proyecto sobre seguridad de la información ante la primera comisión de la asamblea de la ONU, donde se reconoció que "los avances científicos y tecnológicos pueden tener aplicaciones civiles y militares, pero se deben de mantener y fomentar para el desarrollo del progreso científico y tecnológico en bien de las aplicaciones

civiles" (ONU, 1999: 1). Además, este documento ya preveía el desarrollo de las tecnologías a pasos agigantados, el posible uso militar o terrorista, así como para cometer ilícitos.

Por lo anterior, el secretario general de la ONU ha presentado informes anuales con base en los reportes que generan los Estados miembros, respecto del desarrollo en el campo de la información y las telecomunicaciones, en el contexto de la seguridad internacional.

Para 2015 los países que participaron en el *Groups of Governmental Experts* (GGE), convocado por la ONU, "lograron un consenso acerca de las normas, reglas y principios sobre los cuales las naciones tendrían responsabilidades en el ciberespacio; […] establecieron la forma en la cual deberían de cooperar para elaborar e identificar leyes, buenas prácticas, desarrollos y capacitación para contar con un mundo virtual más seguro" (UNODA, s.f.; traducción propia). Los hallazgos más importantes de esta reunión son:

- En el uso de las tecnologías de la información y la comunicación (TIC), los Estados deben observar, entre otros principios, el derecho internacional, la soberanía de los países, la solución de controversias por medios pacíficos y la no intervención en los asuntos internos de otros Estados.
- Las obligaciones en virtud del derecho internacional son aplicables al uso estatal de las TIC; los Estados deben cumplir con sus obligaciones de respetar y proteger los derechos humanos y las libertades fundamentales.
- Los Estados no deben utilizar *proxies* para cometer actos internacionalmente ilícitos que utilicen las TIC y deben procurar que su territorio no sea utilizado por actores no estatales para cometer estos actos. (UNODA, s.f.; traducción propia).

Aun cuando los Estados miembros que conforman la ONU y el EWI están trabajando de manera fuerte en regular el ciberespacio, se nota un avance lento por ambas instituciones, debido quizás a la velocidad con que evoluciona la tecnología, ya que esta va creando nuevos

retos en tiempos cortos que no permiten terminar de analizar los anteriores. Esta situación provoca que dichas instituciones creen múltiples grupos de trabajo que tratan de comprender su impacto; sin embargo, por esta velocidad de cambio no logran más que generar ideas u objetivos que a la vuelta de un año ya no son viables o es necesario analizar nuevamente la situación. En este proceso nunca se llegan a proponer soluciones, o solo quedan en avances cuyo impacto es reducido al reglamentar el uso de Internet.

Aunado a lo anterior y para dar una idea de la evolución de la tecnología, de la inmensidad del problema que es necesario regular y de la falta de normas efectivas que reglamenten el comportamiento en el ciberespacio, Schulman (2016: 32) menciona que estaban conectados y en uso 6,400 millones de dispositivos en todo el mundo en 2016, un 30% más que en 2015; y llegarán a 20,800 millones en 2020. Por otra parte, la industria mundial de ciberseguridad tuvo ganancias de 75,000 millones de dólares en 2015, y se prevé que el mercado crezca a 170,000 millones de dólares en 2020.

Estas situaciones también las visualiza el miembro de la Federación Rusa, Robert Shlegel, quien mencionó:

> Insto en la creación de mecanismos legales internacionales creíbles en el ciberespacio. El modelo de gobernanza de Internet, que actualmente se defiende por las múltiples partes interesadas, es vago e impotente, una imitación de la gobernanza de Internet en lugar de una solución efectiva (McConnell, 2015:13).

CONCLUSIONES.

El motivo por el cual el ciberespacio se está convirtiendo en un campo de batalla, donde los países como Estados Unidos, India, Alemania, Rusia, Afganistán, Corea del Norte y China tienen capacidad real de efectuar ciberataques porque han invertido en crear y desarrollar agencias especializadas para la defensa y ataque del ciberespacio, se debe a lo “económico” que es atacar en este nuevo ámbito virtual, ya que solo es necesario contar con una conexión a Internet, conocimientos técnicos de redes, sistemas operativos, programación, entre otros. Con estos

elementos se puede paralizar uno o varios países, por la simple acción de una serie de códigos de programación especializados en identificar vulnerabilidades, y aprovecharlas para borrar información, encriptar, bloquear el acceso a Internet, tomar el control de uno a varios equipos de cómputo, y todo esto con la seguridad de que es casi imposible identificar al agresor.

Aún queda mucho por hacer en la identificación de los cibercriminales. Quizás ese sea el motivo por el cual no se haya presentado una ciberguerra, porque al no tener la certeza de la fuente de donde se realiza el ataque, las razones y quien o quienes lo financian, no es posible que los Estados declaren una guerra. Pero no cabe la menor duda de que se está trabajando en la identificación del agresor por la cantidad de amenazas que se presentan todos los días (Se puede consultar un mapa en tiempo real de los ciberataques que se presentan todos los días y los países más atacados en Check Point Software Technologies (2017); también se pueden revisar líneas de tiempo de ciberataques desde el año 2011 en Hackmageddon (2016)), y el costo económico (De acuerdo con una publicación de Morgan (2016), el costo de los ciberataques se cuadruplicará en 2019, llegando a $2 trillones de dólares), que implica; también hay esfuerzos como los que realiza el EWI y la ONU en regular y proveer mayor seguridad en el ciberespacio, sin dejar a un lado a la *BSA Software Alliance*, que generó el *EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace* (2015), con la intención de evaluar los avances que han tenido los países de la Unión Europea en temas de ciberseguridad.

LITERATURA CITADA.

Austin, G. (2010). Rights and Responsibilities in Cyberspace: Balancing the Need for Security and Liberty. EastWest Institute. New York: EastWest Institute. Recuperado el 17 de abril de 2017, de https://www.eastwest.ngo/idea/rights-and-responsibilities-cyberspace-balancing-need-security-and-liberty

BSA. The Software Alliance. (2015). EU Cybersecurity Dashboard. Recuperado el 7 de mayo de 2017, de http://cybersecurity.bsa.org/index.html

Check Point Software Technologies. (2017). Live Cyber Attack Threat Map. Recuperado el 25 de mayo de 2017, de https://threatmap.checkpoint.com/ThreatPortal/livemap.html

David Hanson, V. (2010). Génesis de la infantería. En G. Parker (Ed.), Historia de la guerra (J. Gil Aristu, Traductor). Madrid, España: Akal.

Hackmageddon. (2016). Cyber attacks statistics. Recuperado el 15 de mayo de 2017, de http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/

Kushner, D. (2013, febrero 26). The Real Story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program. Recuperado el 23 de mayo de 2017, de IEEE Spectrum: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Lewis, P., & Livingstone, D. (2016a, septiembre 22). Space, the Final Frontier for Cybersecurity? Recuperado el 24 de mayo de 2017, de Chatham House, the Royal Institute of International Affairs: https://www.chathamhouse.org/publication/space-final-frontier-cybersecurity?_ga=2.226081881.2117492801.1495662736-327337264.1493748610

McConnell, B. (2015). Global Cooperation in Cyberspace Initiative. 2016-2017 Action Agenda. EastWest Institute. New York: EastWest Institute. Recuperado el 17 de abril de 2017, de https://www.eastwest.ngo/sites/default/files/ideas-files/ActionAgenda2016_Spread.pdf

Miller, R., & Kuehl, D. (2009, septiembre). Cyberspace and the "First Battle" in 21st-century war. 68 . Washington, D.C., USA: Center for Technology and National Security Policy, National Defense University. Recuperado el 1 de mayo de 2017, de http://ndupress.ndu.edu/Portals/68/Documents/defensehorizon/DH-68.pdf?ver=2014-03-06-114910-860

Morgan, S. (2016). Cyber Crime Costs Projected To Reach $2 Trillion by 2019. Recuperado el 10 de mayo de 2017, de Forbes: https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6a127c33a913

Nagorski, A. (2010). EWI 's 2009 Annual Report. EastWest Institute. New York: EastWest Institute. Recuperado el 10 de mayo de 2017, de https://www.eastwest.ngo/sites/default/files/ideas-files/EWI2009.pdf

ONU. (1999). Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional. Organización de las Naciones Unidas, Asamblea General. New York: ONU. Recuperado el 15 de mayo de 2017, de http://undocs.org/es/A/RES/53/70

Rauscher, K., & Yaschenko, V. (2011). Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations. New York: EastWest Institute and the Information Security Institute of Moscow State University. Recuperado el 16 de mayo de 2017, de https://www.eastwest.ngo/idea/russia-us-bilateral-cybersecurity-critical-terminology-foundations

San Pedro, P. (2015, march 26). Siria: orígenes y causas del conflicto. recuperado el 24 de amyo de 2017, de El diario.es: http://www.eldiario.es/desigualdadblog/Siria-origenes-causas-conflicto_6_370672945.html

Schulman, A. (2016). Annual Report 2015. EastWest Institute. New York: EastWest Institute. Recuperado el 23 de mayo de 2017, de https://www.eastwest.ngo/sites/default/files/ideas-files/EWIAnnualReport_2015.pdf

Stern, S. (2013). Annual Report 2012. EastWest Institute. New York: EastWest Institute. Recuperado el 25 de mayo de 2017, de https://www.eastwest.ngo/sites/default/files/ideas-files/ewi-2016-annual-report_0.pdf

UNODA. (s.f.). Developments in the field of information and telecommunications in the context of international security. Recuperado el 26 de mayo de 2017, de United Nations Office for Disarmament Affairs: https://www.un.org/disarmament/topics/informationsecurity