INSTITUTO DE INVESTIGACIONES ESTRATÉGICAS DE LA ARMADA DE MÉXICO

DO 22/18
05/10/18

Capitán de Navío
Vladimir Delgadillo Martínez

El ciberespacio, un facilitador de riesgos

RESUMEN

El presente artículo versa sobre la importancia del ciberespacio en un mundo globalizado, advirtiendo algunos de los factores de riesgo que existen en el entorno virtual a causa de la conectividad múltiple que necesita una sociedad digitalizada. Por lo anterior, es necesario conocer y prevenir estos factores de riesgo, para establecer protocolos, planes y procedimientos de emergencia, los cuales integren una adecuada gestión de riegos, que permitan contener las amenazas y evitar daños en la infraestructura crítica.

También se exponen algunas ideas generales para fortalecer los marcos jurídicos, políticas y estrategias nacionales que proporcionen la resiliencia cibernética gubernamental, por tanto, se colabore en el establecimiento de una legislación internacional que coadyuve a implementar una gobernanza del ciberespacio y consecuentemente, se fortalezca la seguridad internacional fundamentada en conceptos y valores que garanticen un internet seguro y libre.

Palabras claves: Ciberespacio, internet, conectividad, factor de riesgo, datos, información, ciberterrorismo, cibercrimen, ciberdelincuencia

ABSTRACT

This article deals with the importance of cyberspace in a globalized world, noting some of the risk factors that exist in the virtual environment due to the multiple connectivity that a digital society needs. Therefore, it is necessary to know and prevent these risk factors, to establish protocols, plans and emergency procedures, which integrate an adequate management of risks, which allow to contain the threats and avoid damage to the critical infrastructure.

Some general ideas are also exposed to strengthen the legal frameworks, policies and national strategies that provide government cyber resilience, therefore, collaborate in the establishment of an international legislation that helps to implement a cyberspace governance and consequently, strengthens the security international based on concepts and values that guarantee a safe and free internet.

Key words: Cyberspace, internet, connectivity, risk factor, data, information, cyberterrorism, cybercrime, cybercrime

INTRODUCCIÓN

Se define como ciberespacio al "ámbito artificial creado por medios informáticos" (RAE, 2018), otra definición importante de razonar es la que proporciona Allan Collins (2016) que cita "Ciberespacio connota la fusión de todas las redes de comunicación, bases de datos y fuentes de información en un vasto, enmarañado y diverso bloque de intercambio electrónico" (p.401). En nuestro país la Estrategia Nacional de Ciberseguridad (ENCS) dice que "es un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas y permite el ejercicio de sus derechos y libertades como lo hacen en el mundo físico" (gob.mx, documentos, 2017, pág. 27).

Analizando las definiciones anteriores y desde un punto de vista conceptual, es importante aclarar que el Internet y el ciberespacio son entes diferentes, considerándose al primero como la parte técnica -la infraestructura- que proporciona los medios para que exista e interactúe el segundo, el cual interconecta o almacena todo el contenido –información–, permitiendo relacionar a las personas, organizaciones, sociedades y gobiernos para interactuar desde el mundo real al mundo virtual y viceversa, ocasionando un nuevo concepto polisémico del lenguaje que antepone el termino ***ciber***, por ejemplo: cibernético, cibernauta, ciberdefensa, ciberataque, ciberamenaza, ciberseguridad, cibercrimen, ciberdelincuente, cibercomunidad, etc.

El ciberespacio es actualmente el medio más rápido de comunicar o transmitir información por diversas formas como audio, datos, imágenes, videos e información escrita en formato digital, lo que ocasiona –de acuerdo al tipo de información o mensaje transmitido– afectaciones que pueden ser positivas o negativas. Los recursos que contiene el internet propician que el ciberespacio tenga un ambiente multidimensional, considerándose como un ESPACIO UNIVERSAL COMÚN que no tiene dueño y en donde los límites entre lo público y lo privado se diluyen rápidamente.

La disolución de las fronteras en el Ciberespacio afecta a las personas, las organizaciones y también a los gobiernos, debido a que en el presente siglo se ha generado en el mundo una dependencia informática, requiriendo una *elevada conectividad*[1] debido a: los nuevos dispositivos tecnológicos, a los sistemas informáticos que necesitan compartir e intercambiar datos, la cantidad de usuarios que se incrementan día a día y a la considerable cantidad de datos que se almacenan en las diversas plataformas, servidores y bases de datos gubernamentales, empresariales, educativas, de investigación o particulares, por citar algunas.

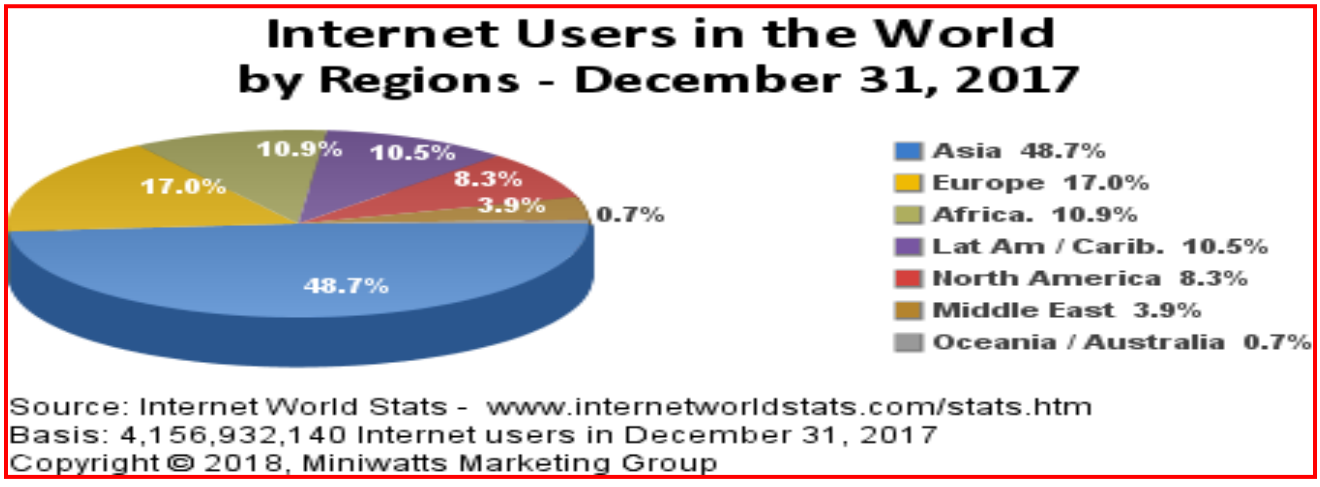
[1] Algunos autores la denominan como híperconectividad, término establecido para designar los distintos medios de comunicación que las personas utilizan como: teléfonos inteligentes, tabletas, computadoras personales, correo electrónico, servicios de mensajería instantánea, redes sociales, etc.

Esta enorme cantidad de datos se incrementa en forma exponencial, originando la necesidad de crear un sistema que facilite el almacenamiento, la búsqueda y el procesamiento de la información, lo que provoca que la información sensible como datos personales, datos bancarios o datos biométricos sean vulnerables, haciendo del ciberespacio un factor de riesgo para las personas, las organizaciones privadas, las sociedades y para los gobiernos.

El *Big Data*[2] es el término con el que se define a la enorme cantidad de datos almacenados en medios informáticos y que pueden estar disponibles en el ciberespacio por medio de software especializado. El *Big Data* proporciona la ventaja de armonizar datos –estructurados o no estructurados–, con aplicaciones digitales -software o apps- o con un gestor de administración informático, que puedan ser empleados desde diversas plataformas como computadoras, tabletas, teléfonos inteligentes, redes sociales, buscadores de internet, videojuegos, etc., por lo que el sector empresarial lo "considera la tendencia clave…del futuro, y las empresas quieren utilizar la gran cantidad de datos que producimos…para adaptar sus estrategias de marketing [aunque puede ser implementado en cualquier disciplina, área o campo del poder] a través de la publicidad personalizada y la predicción del comportamiento del consumidor futuro" (Collins, 2016).

El ciberespacio es un recurso empleado en todo el mundo y de acuerdo a los datos citados por Octavio Islas, el cual externa que "la Internet World Status (IWS) publicó la más reciente actualización de sus estadísticas de la penetración mundial de internet…estimó 3,731,973,423 son usuarios de Internet" (Islas, 2017); lo anterior fundamenta que el ciberespacio sea considerado como un espacio global (ver imagen No. 1) y de acuerdo con esta necesidad de conectividad sea considerado como un dominio que permite eficientar el desempeño laboral, familiar e interpersonal, pero también sea conceptuado como un facilitador de riesgos para una sociedad altamente digitalizada.

Imagen No. 1: Gráfica por regiones de usuarios de Internet en el mundo



Fuente: obtenida de **https://www.internetworldstats.com/stats.htm**

[2] Su traducción sería *Macrodatos* el cual hace referencia a una cantidad de datos capturados que supera la capacidad de los software para administrarlos y procesarlos en un tiempo óptimo para su análisis y posterior evaluación.

Desarrollo

Actualmente las sociedades en todo el mundo se hacen cada día más dependientes del Ciberespacio, una zona donde pueden converger diversas vulnerabilidades, debido a que cualquier persona que tenga acceso a la red informática mundial (conocida comúnmente como www, acrónimo de la expresión inglesa *World Wide Web*) podría obtener información sensible que atente contra la privacidad de las personas o la seguridad de organizaciones y de los gobiernos.

Los medios empleados como el correo electrónico, las redes sociales (*Twitter, Facebook, WhatsApp, Instagram, Youtube, Snapchat, Skype*, etc.), servicios como el *File Transfer Protocol,* el cual es un protocolo de transferencia de archivos entre sistemas conectados a una red con una arquitectura cliente-servidor (FTP), *Telecommunication Network*, nombre de un protocolo de red empleado para tener acceso remotamente a una computadora (Telnet) o *Gopher* antecesor de la www, el cual fue un programa empleado para organizar y mostrar información (creado por la Universidad de Minnesota en 1991), hacen que el Ciberespacio sea multidimensional y multiusuario, teniendo contacto en forma sincrónica o asincrónica.

La forma de acceso a la www se efectúa por medio del *Uniform Resource Locator* (URL), cuya traducción literal es localizador uniforme de recursos o dirección de internet, el cual es el medio para obtener una dirección única para ir a un recurso específico ubicado en la red, la cual emplea un medio denominado buscador –llamado también navegador como *google, safari, internet explorer, mozilla, opera*, etc.– el cual busca la información o ejecuta el servicio en los diversos servidores a que tenga acceso de acuerdo al protocolo *Internet Protocol (*IP), que es un identificador único asignado a cada equipo que se conecta a la red, para administrar las autorizaciones a programas y software, así como gestionar claves o permisos de acceso a la web.

El propósito de explicar lo anterior es para visualizar lo complejo, pero al mismo tiempo la simpleza de acceso a la información, datos personales, datos biométricos, recursos tecnológicos, recursos financieros o programas oficiales de organizaciones civiles, dependencias estatales y sistemas de seguridad del gobierno. Es por esto, que hoy en día se han incrementado las vulnerabilidades y riesgos, generando afectaciones negativas que son vinculadas con una serie de actividades ilícitas necesarias de contener, para así implementar políticas de control del Ciberespacio sin limitar la libertad de expresión democrática. Por lo anterior, se consideran los siguientes riesgos y vulnerabilidades en el uso y empleo del ciberespacio que puede llegar a afectar en la seguridad nacional:

Político y social. El ciberespacio es un lugar donde existe interacción humana, creando un espacio virtual que puede ocasionar inherentemente afectaciones en la sociedad en los aspectos económicos, políticos, sociales, tecnológicos, medioambientales y militares entre otros.

Desde el punto de vista Político-Social los principales riesgos y vulnerabilidades se dan debido a la desinformación y la manipulación de la información, con el fin de tener acceso a datos personales, a cuentas bancarias o influir en procesos democráticos como las elecciones, quedando demostrado recientemente en los casos de presunta injerencia de la Federación Rusa en las elecciones de los Estados Unidos de América (EE. UU.) y en el referéndum del BREXIT en el Reino Unido.

Estas presuntas intrusiones de Rusia indujeron cambios en las relaciones de los individuos con el gobierno, afectando las estructuras del poder y provocando el empoderamiento del individuo que con los conocimientos técnicos-profesionales y los equipos informáticos adecuados, ejerce distintos grados de influencia y cambios en la percepción de la sociedad a la que se dirigen los mensajes.

Un punto importante de considerar para comprender el grado de influencia que se puede llegar a generar en una sociedad –como sucedió con la Primavera Árabe en el 2011 y el movimiento ciudadano *Yo soy 132* en México– lo brinda el dato estadístico proporcionado por la IWS (ver imagen No. 1), el cual estima se incrementen los usuarios de internet en el mundo, debido a la velocidad con las que evolucionan las telecomunicaciones y se continúe con la automatización de sistemas empleados en intercambios comerciales, económicos, servicios de salud, aseguradoras, instituciones educativas, así como en todas las actividades que vinculan y soportan las actividades de los individuos.

Conflicto armado. La seguridad del Estado es un objetivo fundamental de cualquier nación, siendo importante la actualización y modernización de los recursos, así como de la tecnología militar. Arturo Sarukhán[3] expresa que "El Internet y las redes sociales son el nuevo campo de batalla geopolítico" (2018), por lo que después de la guerra fría, se considera que actualmente existen más tensiones en el mundo a causa de la explotación de los recursos cibernéticos, los cuales afectan la seguridad y el poder militar de una manera más económica que un conflicto tradicional.

La primera guerra del Golfo Pérsico fue "la primera vez que se presenciaba televisado en directo un ataque bélico" (Courel, 2013), en la segunda Guerra del Golfo se consideró "que era una guerra televisada en directo" (Courel, 2013), en ambos conflictos la televisión era el medio de difusión más relevante, transmitiéndose principalmente lo que a los EE. UU. le interesaba o le convenía. Sin embargo, actualmente el uso de todos los recursos del ciberespacio, ha permitido transmitir de forma masiva eventos que antes se censuraban o no convenía a los gobiernos difundir, tal es el caso del ataque con armas químicas a la población de Siria, las pruebas nucleares efectuadas por Corea del Norte y el empleo de las redes sociales por parte del ejército de Israel como lo expresa Maite Garrido (2013) en donde *Twitter* fue usado para transmitir la muerte del dirigente de HAMÁS[4] Ahmed Jabari (Courel, 2013).

[3] Es diplomático y consultor internacional. Nacido en la Cd. de México, en 1963, designado Embajador de México en Estados Unidos del 2007 al 2013.
[4] Movimiento de Resistencia Islámica en contra de la ocupación israelí de Cisjordania y la Franja de Gaza, considerada por EE.UU. e Israel como una organización terrorista.

Otro de los riesgos que producen las redes sociales en los conflictos armados fue el caso de *Wikileaks*, el cual consistió en la filtración de documentos militares correspondientes a las guerras de Irak y Afganistán, vulnerando así los servicios de Inteligencia del gobierno en los EE.UU.

Imagen No. 2: (izquierda) UAV artillado con misiles Hellfire, (derecha) estación de control de UAV´s.

Fuentes: https://parrotnews.wordpress.com/2011/10/14/us-drone-strike-kills-78-in-somalia/ y https://elpais.com/internacional/2012/07/30/actualidad/1343674302_759363.html

Una vulnerabilidad que hasta el momento existe pero no se ha visto afectada, es el ataque a sitios estratégicos mediante los UAV´s[5] armados con misiles (imagen No. 2 izquierda), los cuales son controlados a control remoto contra objetivos de alto valor estratégico, como en el caso de Somalia, donde EE. UU. atacó un campo de entrenamiento dejando aproximadamente 150 muertos de la organización radical islamista *Harakat al-Shabaab al-Muyahidin* (BBC, 2016).

Los UAV´s tienen sistemas informáticos avanzados, operados desde tierra por una estación de control (imagen No. 2 derecha) que se enlaza mediante un sistema *Data Link*[6], poseen además un sistema de control automático de vuelo que, en caso de romperse el enlace, puede recalcular su trayectoria para retornar a la base o sitio desde donde fue lanzado.

Existen actualmente desarrollos con tendencias a implementar en los UAV´s inteligencia artificial, para permitir ejecutar toma de decisiones y así hacer más eficiente sus ataques selectivos. Sin embargo, estos sistemas pueden ser afectados por armas de impulsos magnéticos o sus sistemas podrían ser vulnerados por hackers[7] o ciberataques, que tomen el control evitando los procesos de autodestrucción, direccionando sus misiones en contra de las propias fuerzas armadas o para cometer agresiones sobre poblaciones civiles u otros objetivos.

[5] Acrónimo del inglés Unmanned Aerial Vehicle, que significa Vehículo Autónomo No Tripulado. Estos equipos son desarrollados en gran cantidad de fuerzas armadas en el mundo, debido a las ventajas que proporciona su empleo estratégico y se consideran una ventaja en futuros conflictos, debido a la versatilidad en su uso.
[6] Es un dispositivo para establecer un Enlace de Datos, que permite transmitir y recibir información.
[7] La definición que proporciona el diccionario Cambridge dice que es la persona que usa ilegalmente una computadora para acceder a la información almacenada en otro sistema informático o para propagar un virus informático (traducción propia).

Por lo anterior, debido a la importancia tecnológica en el empleo de estos dispositivos, *Ben Knight* perteneciente a la cadena periodística alemana *Deutsche Welle* (DW), elaboró en el 2017 una pequeña guía sobre el mundo de los drones militares[8], citando que "apenas han comenzado a explotar todas las posibilidades que ofrecen los vehículos aéreos de combate no tripulados" (Knight, 2017).

Dentro de la clasificación que hace Ben Knight, menciona los drones grandes de combate y vigilancia como el *MQ-1 Predator* y el *MQ-9 Reaper*, los cuales son desarrollados por la empresa *General Atomics*; también considera al *Global Hawk*, fabricado por *Northrop Grumman,* todos utilizados por las fuerzas armadas de los EE.UU., de los cuales el *MQ-9 Reaper* "cuesta más de US$16 millones la unidad y Estados Unidos opera alrededor de 100 de ellos, a través de varias agencias" (BBC, 2018). Las capacidades más notables es que puede ser armado con misiles aire-tierra y con misiles guiados por láser, por lo cual, en caso de sufrir un *hackeo*, puede quedar a disposición de los ciberdelincuentes una herramienta con capacidades militares que represente una amenaza o riesgo a poblaciones, instalaciones estratégicas o a las propias fuerzas armadas de cualquier gobierno.

Un ejemplo de lo anterior, es el caso citado en la BBC Mundo (2018) en julio pasado, donde una persona (*hacker*) acceso a un equipo de cómputo y extrajo información confidencial que tenía manuales de mantenimiento y guías de entrenamiento, mismas intento vender en la *Deep Web* (internet Profunda):

> El hacker accedió a la computadora de un capitán de la Fuerza Aérea Estadounidense y robó información confidencial sobre estas naves, lo cual fue confirmado por la compañía de ciberseguridad Recorded Future. Entre los archivos secretos, fueron revelados manuales de mantenimiento del dron MQ-9 Reaper, así como varias guías de entrenamiento para tropas que Estados Unidos tiene desplegadas en países del extranjero. Aunque la policía dijo que ninguna de la información robada califica como "clasificada", sí estaba sujeta al control y uso estricto del gobierno estadounidense (BBC, BBC Mundo, 2018)

Con base en lo anterior, se establece que el factor de riesgo que representa el ciberespacio para los gobiernos que tienen UAV´s artillados o los futuros desarrollos que proyectan el empleo de la inteligencia artificial considerados como armamento estratégico, se puede convertir en una amenaza latente si no se establecen políticas de control, procedimientos y sistemas de gestión de crisis adecuados para el control y operación de estos equipos, así como de la información almacenada en el *Big Data* o compartida –publicada- en la internet.

Terrorismo. La Oficina de las Naciones Unidas contra la droga y el delito (UNDOC[9]) externa que el empleo del Internet y del Ciberespacio con fines terroristas "es un fenómeno que se propaga con rapidez y

[8] Para más información de esta guía puede consultarse el siguiente vínculo https://p.dw.com/p/2fVYx
[9] La United Nations Office on Drugs and Crime (UNDOC), es un organismo de la ONU y líder mundial en la lucha contra las drogas ilícitas y la delincuencia internacional, tiene a su cargo el programa contra el terrorismo. Fue establecida en 1997 y tiene su sede en Viena

exige una respuesta dinámica y coordinada de los Estados Miembros" (UNDOC, 2013), por lo que desarrolla instrumentos jurídicos[10], para evitar el empleo del Ciberespacio con fines terroristas.

El fenómeno del Terrorismo se ha convertido en una amenaza en el Ciberespacio que evoluciona rápidamente, debido a ser un medio de comunicación que es "sumamente dinámico, que llega a un público cada vez mayor en todo el mundo. El desarrollo de tecnologías cada vez más sofisticadas ha creado una red con un alcance verdaderamente mundial y barreras al acceso relativamente bajas" (UNDOC, 2013). Esta es la razón por la que se considera un factor de riesgo que ha logrado globalizarse y propagarse, mediante la internet, convirtiéndose así en una amenaza transnacional que emplea según la UNDOC (2013, p. 3) seis categorías o recursos del Ciberespacio:

La propaganda: en este rubro se incluyen aspectos como el reclutamiento, la radicalización y la incitación al terrorismo, empleado principalmente audios y videos para poder difundir su ideología con una constante retórica de auto justificación. Actualmente también difunden en formato digital revistas, libros, folletos, logros y presentaciones que promueven la violencia, mediante redes sociales como Facebook, Twitter, YouTube y Rapidshare.

La financiación: consistente en la captación de recursos económicos para sostener sus operaciones y sus actividades, generalmente proveniente de personal partidario, cooptado, reclutado o de Estados y gobiernos que apoyan por intereses mutuos sus acciones. La recaudación puede ser de cuatro tipos generales, la recaudación directa, comercio electrónico, empleos de pago en línea -PayPal o Skype- y contribuciones a organizaciones benéficas.

El adiestramiento: en este punto se consideran las necesidades logísticas para capacitar al personal reclutado e iniciar su radicalización, como la compra de armamento y explosivos; vestuario, comida, alojamiento, vehículos y recursos tecnológicos necesarios en unos campamentos de adiestramiento alternativos de terroristas. Existen también campamentos virtuales terroristas que emplean las diversas plataformas para difundir archivos multimedia de cómo fabricar armas o explosivos, asesorar la planeación y ejecución de ataques terroristas, así como proporcionar herramientas para realizar acciones de inteligencia, contrainteligencia y piratería de los servicios de comunicación en la red.

La planificación: acciones dedicadas a la obtención de información de dominio público, enlaces de comunicaciones y cualquier contenido que permita fortalecer las capacidades para efectuar un acto terrorista. La implicación de un acto terrorista considera el uso de medios de comunicación a distancia que pueden estar cercanos o lejanos, incluso en otros países o continentes con el objetivo de promover el extremismo violento. Es de esta forma que también pueden efectuar la selección de objetivos de interés o de alto valor estratégico, gracias a que el internet y el ciberespacio difuminan las fronteras.

[10] Por acuerdo de la Asamblea General de la ONU en su resolución 66/178 del 2011.

La ejecución: el empleo del ciberespacio y del Internet permiten efectuar coordinaciones previas a la ejecución de un acto terrorista, tener contacto con sus personas objetivos o incluso pueden transmitir en tiempo real sus acciones de violencia extrema. Es de esta manera que los grupos y organizaciones terroristas pueden adquirir materiales requeridos usando el comercio electrónico, logrando disminuir costos logísticos y manteniendo el anonimato.

Los ataques cibernéticos: denominados comúnmente ciberataques, los cuales permiten el uso indiscriminado de las redes y medios informáticos; así como de las fuentes del ciberespacio y de los recursos del internet. Son principalmente dirigidos a organizaciones, sitios oficiales o individuos elegidos previamente y analizando sus vulnerabilidades, como computadoras, servidores o infraestructura complementaria, empleando códigos maliciosos, virus informáticos, piratería, phishing o cualquier tipo de acceso no autorizado. Una característica general de los ciberataques terroristas, es que se enfoca o dirige con el propósito de infundir terror en la sociedad, por lo que buscan afectar los sitios públicos u oficiales del gobierno como uno de sus objetivos políticos.

Con la información anterior, se determina que el factor de riesgo que ocasiona el ciberterrorismo afecta a cualquier país y en cualquier nivel de gobierno -federal, estatal o municipal-, para evitar esta situación es necesario fortalecer los marcos jurídicos, como ejemplo de esto, en la cámara de diputados del congreso de México, desde enero del presente año, se presentó una iniciativa de ley para:

> Reformar el código penal federal para imponer pena de prisión de 15 a 40 años y **400 a mil 200 días multa** a quienes incurran en **"ciberterrorismo"**, o el uso de las tecnologías de la información para causar temor, daño o intimidar a personas o grupos sociales (Morales, 2018).

El artículo 139 del código penal federal, establece esta pena –prisión de 15 a 40 años– por cometer el delito de terrorismo, definiendo este término en su fracción II de la siguiente forma: "Al que acuerde o prepare un acto terrorista que se pretenda cometer, se esté cometiendo o se haya cometido en territorio nacional" (DOF, 1931 reforma 2018). Con esta iniciativa[11] se trata de anexar el término ciberterrorismo y evitar que las infraestructuras críticas nacionales tengan disrupciones[12] en los distintos servicios que proporciona el gobierno, como la energía eléctrica, agua potable, sistemas de transporte -como el metro de la ciudad de México y los aeropuertos-, las telecomunicaciones -satelitales y de radiofrecuencia-, sistema de salud pública, los servicios financieros, etc., que representen un riesgo o amenaza a la población, afecten la gobernabilidad o desestabilicen al Estado.

Crimen organizado. este fenómeno social ha evolucionado ampliamente haciendo uso de las tecnologías para asociarse y cometer delitos de alto impacto, diversificando sus actividades (pornografía, trata de personas, lavado de dinero, venta de armas, drogas y estupefacientes, extorsiones, fraudes, etc.),

[11] La cual a la fecha de elaboración de este documento se encuentra en calidad de pendiente de resolución.
[12] Termino empleado para definir interrupciones inesperadas provocadas por ciberataques a infraestructura crítica.

debido a la facilidad de acceso al internet, el anonimato que éste proporciona y el uso de todos los recursos propios del Ciberespacio, haciendo que sea uno de los aspectos más importantes de atender por los gobiernos por las afectaciones que representa al Estado de Derecho.

El empleo de las Tecnologías de la Información y la Comunicación (TIC´s) facilitan la convivencia, permite eficientar el trabajo de las personas y simplifica también la consulta de la información, así como el empleo de recursos tecnológicos a los gobiernos, sin embargo; también ocasiona diversos factores de riesgos, que cuando son utilizados por el crimen organizado, pueden llegar a convertirse en amenazas muy serias para los gobiernos.

La principal ventaja que les proporciona el ciberespacio a las organizaciones criminales, es el empleo del anonimato (ver imagen No. 3) para cometer ilícitos y adoptar conductas sociales que afectan la gobernabilidad –capacidad de gobernar– y la gobernanza –promoción en la participación y responsabilidad de la sociedad para mantener el estado de derecho–. Por lo anterior, se hace indispensable que todos los gobiernos adapten, desarrollen e implementen respectivamente sus marcos jurídicos nacionales, sus políticas de seguridad nacional y las estrategias de ciberseguridad.

Imagen No. 3: Representación del Anonimato en el Ciberespacio.

Fuente: http://www.elfinanciero.com.mx/economia/pagos-electronicos-presentarian-lentitud-tras-ciberataque-bancos

Considerando la gran cantidad de datos e información que se almacenan en los servidores de las dependencias gubernamentales, instituciones bancarias y los servicios de salud, los cuales frecuentemente están disponibles a los cibernautas para hacer consulta de datos o diversos trámites oficiales y particulares, hace que esta información pueda ser obtenida por el crimen organizado vulnerando la seguridad y produciendo grandes repercusiones.

Un caso reciente es el ataque cibernético sucedido en México, el cual afectó las transacciones realizadas por el sistema de pagos electrónicos interbancarios (SPEI), como cita Jeanette Leyva (2018) del Periódico el Financiero “tras el intento de ciberataque…los bancos operan el SPEI con el programa de contingencia, lo

que vuelve más lentas las transacciones" (Leyva, 2018). Este incidente cibernético costo aproximadamente 300 millones de pesos, según la fuente oficial de Banco de México (BANXICO).

La Doctora Gema Sánchez Medero en su artículo Ciberespacio y el Crimen Organizado, los Nuevos desafíos del siglo XXI (2012), cita la definición proporcionada por Rodríguez Bernal (2007) donde define al cibercrimen de la siguiente manera:

> El Cibercrimen abarca desde el delito económico, como el fraude informático, el robo, la falsificación, el computer hacking, el espionaje informático, el sabotaje, la extorsión informática, la piratería comercial y otros crímenes contra la propiedad intelectual, la invasión a la intimidad, la distribución de contenidos ilegales y dañosos, la incitación a la prostitución y otras actitudes que atenten contra la moralidad, y el crimen organizado (p. 73).

Esta definición permite comprender la gran multiplicidad de acciones en las que el crimen organizado utiliza el ciberespacio para cometer actividades delictivas, a fin de alcanzar su principal propósito que es la obtención de recursos económicos por diversas fuentes; así como otros objetivos secundarios como el lavado de dinero empleando el comercio electrónico, desacreditar a instituciones gubernamentales, bloquear o modificar páginas web o simplemente propagar virus informáticos en forma de *malware*.

En la ENCS (gob.mx, 2017) se cuenta con dos términos importantes de mencionar, la ciberdelincuencia y delitos cibernéticos o ciberdelitos, los cuales quedan definidos de la siguiente manera:

> Ciberdelincuencia. Actividades que llevan a cabo individuo(s) [que] realiza(n) [o] que utilizan como medio o como fin a las tecnologías de la información y comunicación (p. 27).
>
> Delitos cibernéticos o ciberdelitos. Acciones delictivas que utilizan como medio o como fin a las tecnologías de la información y comunicación y que se encuentran tipificados en algún código penal u otro ordenamiento nacional (p. 28).

Con lo anterior, se infiere que existe un vacío –legal– en la primera definición, debido a que se generaliza a la ciberdelincuencia como cualquier actividad realizada o efectuada con TIC´s, lo que ocasiona una confusión en la interpretación del término y al mismo tiempo un debilitamiento del marco jurídico, sin embargo, la definición de ciberdelitos queda clara y sustentada en una legislación sólida y vigente, debido a que considera cualquier acción delictiva contemplada en algún ordenamiento nacional.

Estas discordancias que observamos en nuestra legislación nacional, puede suceder en cualquier país, por lo que se convierten en amenazas a los gobiernos y en oportunidades para el crimen organizado, el cual aprovecha los resquicios legales para adaptarse, evolucionar y buscar nuevas formas de comprometer el estado de derecho. También esta situación de ausencia o falta de alineamiento de los marcos jurídicos nacionales, imposibilitan la oportunidad de crear una legislación internacional que fortalezca la lucha contra el crimen organizado y permita tomar acciones coordinadas para incrementar la seguridad internacional de

una forma multidimensional, donde se considera que la proposición debe estar basada en cuatro conceptos: «la confianza, cooperación, acción y responsabilidad recíproca».

Para reducir las brechas legales en nuestro país que le brindan ventaja al crimen organizado, en mayo del presente año el consejo ejecutivo de la comisión intersecretarial para el desarrollo del gobierno electrónico (CIDGE) del gobierno federal "robusteció la Estrategia Nacional de Ciberseguridad [ENCS] con el objetivo de salvaguardar los aplicativos e infraestructura y favorecer la cultura tecnológica de la seguridad" (gob.mx, CIDGE, 2018), medidas dirigidas principalmente a procesos aplicativos y la infraestructura crítica.

En otro contexto, se debe priorizar la cultura de prevención ante el cibercrimen, pero también es importante establecer lo siguiente: un sistema de gestión de crisis, planes de contingencia y los procesos de continuidad a las operaciones en caso de ataques cibernéticos, debido a que como cita *Collins* (2016), "El control de la información está guiado por la gestión del riesgo, que consiste esencialmente en aceptar que uno es (o permanece) inseguro: el nivel de riesgo nunca puede reducirse a cero (p. 411, traducción propia). Considerando la relevancia que toma la gestión de riesgo, el CIDGE en su primera sesión extraordinaria "reiteró que el Centro Especializado en Respuesta Tecnológica (CERT-MX) ante cualquier amenaza cibernética que ponga en peligro la infraestructura tecnológica del Estado, procede conforme al protocolo de gestión de incidentes para prevenir afectaciones a instituciones mexicanas" (gob.mx, CIDGE, 2018).

Reflexionando lo anterior, se puede considerar que el ciberespacio por naturaleza es inseguro (ver imagen No. 4), siempre existirá un nivel de riesgo aunque se cuenten con las herramientas y medidas de seguridad en su utilización, debido a que los *hacker* que son cooptados por el crimen organizado para cometer ciberdelitos, cuentan con al menos dos recursos importantes para romper las barreras de seguridad informáticas que son dinero y tiempo.

Imagen No. 4: Representación gráfica de los factores de riesgo existentes en el ciberespacio.

Fuente: imagen obtenida de http://guides.ll.georgetown.edu/cyberspace

Conclusiones

Al utilizar la internet y el ciberespacio, existen considerables factores de riesgo, los cuales pueden llegar a convertirse en vulnerabilidades o amenazas si no se establecen medidas de control, fundamentos jurídicos, políticas de seguridad y sobre todo sensibilización de los usuarios para proteger sus sistemas, sus datos personales y su propia seguridad personal.

El ciberespacio es un ámbito artificial que fusiona las redes de comunicación, datos e información en un entorno digital, en el cual interactúan las personas con su contenido, pasando del mundo real al mundo virtual. Por lo anterior, es el medio más rápido de comunicar o transmitir información, ocasionando afectaciones que pueden ser positivas o negativas, considerándose un entorno multidimensional, multiusuario, así como un espacio global donde no existen fronteras y sus afectaciones benefician o perjudican a todos los usuarios, sean personas, empresas, organizaciones o gobiernos.

La dependencia informática ocasiona la necesidad de una híperconectividad, que permita compartir e intercambiar datos e información de las diversas plataformas y recursos en donde se encuentren almacenados, así se crea el *Big Data,* el cual administra, procesa, analiza y evalúa datos e información, para así poder predecir comportamientos futuros. Sin embargo, esta situación provoca que el ciberespacio se considere un facilitador de riesgos para un mundo y una sociedad digitalizada, en donde se prevé que los futuros conflictos se darán por el control del ciberespacio y sus recursos.

La digitalización de datos personales, financieros, biométricos, información clasificadas de desarrollos tecnológicos y militares entre otros, incrementa los riesgos, provocando una serie de actividades ilícitas o conductas criminales, las cuales son necesarias de contener mediante políticas y estrategias de control, sin que esto límite la libertad de expresión. Los riesgos y amenazas pueden ser originadas por las siguientes causas: político y social, conflictos armados, terrorismo o el crimen organizado.

El ciberespacio ha cambiado las estructuras del poder, empoderando a individuos con conocimientos técnicos-profesionales que ejercen distintos grados de influencia en la sociedad, modificando la percepción de seguridad y convirtiéndolo en un nuevo dominio de la guerra, dando lugar a conceptos como ciberguerra, ciberoperaciones, ciberinteligencia, ciberdefensa y otros más.

Los desarrollos tecnológicos militares poseen sistemas informáticos avanzados, incluso algunos con posibilidad de integrar inteligencia artificial, los cuales pueden ser blanco de ciberataques y la posibilidad de que ciberterroristas obtengan el control de estos equipos, con los riesgos que esto conlleva para cualquier gobierno.

Asimismo, la ciberdelincuencia también ha evolucionado, capacitándose y tecnificándose, por lo que sus actividades ilícitas se diversifican aprovechando los recursos del internet y sobre todo el anonimato que es

una de las ventajas más importantes que les proporciona el ciberespacio. Los gobiernos y la sociedad tienen la necesidad de intercambiar datos e información en diversas plataformas tecnológicas, por lo que permite a los cibernautas tener acceso a bases de datos o al *Big data*. Estas circunstancias crean la necesidad de actualizar los marcos jurídicos, las políticas y las estrategias de ciberseguridad para fortalecer el Estado de derecho, evitando poner en riesgo la seguridad nacional.

La homologación de terminología en la legislación nacional, es un aspecto importante para el fortalecimiento del Estado de derecho, porque a causa de las discrepancias o imprecisiones que existen provocan que los ciberdelincuentes no sea sancionados o queden impunes, debido a que algunas de sus actividades ilícitas no se encuentran contempladas en las leyes, códigos y reglamentos nacionales, quedando como una asignación pendiente de efectuar.

Por último, el fortalecimiento de los marcos jurídicos, permitirá coadyuvar en la elaboración de una legislación internacional, que permita realizar acciones coordinadas basadas en la confianza y la cooperación, solo así se logrará incrementar la seguridad cibernética internacional (ver imagen 5), siempre y cuando los gobiernos estén dispuestos a actuar con una responsabilidad recíproca.

Imagen No. 5: Representación de la seguridad cibernética internacional.

Fuente: http://chicoseduca2lareencarnacion.blogspot.com/2015/11/escuelas-ciberneticas.html

BIBLIOGRAFÍA

BBC. (12 de jul de 2018). *BBC Mundo.* Obtenido de Noticias, Redacción: https://www.bbc.com/mundo/noticias-44813793

BBC, N. (7 de Julio de 2016). *BBC.* Obtenido de News, Mundo, Noticias: http://www.bbc.com/mundo/noticias/2016/03/160307_eeuu_somalia_al-shabab_drones_az

Collins, A. (2016). *Contemporary Security Studies.* UK: Oxford.

Courel, M. a. (10 de septiembre de 2013). *El Diario.* Obtenido de Diario Touring. Guerra en la era de las redes sociales: https://www.eldiario.es/turing/Nuevas-tecnologias-tiempos-guerra_0_172183356.html

DOF. (14 de agosto de 1931 reforma 2018). *H. Cámara de Diputados.* Obtenido de Codigo Penal Federal: http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo83048.pdf

gob.mx. (13 de nov de 2017). *documentos.* Obtenido de Estrategia Nacional de Ciberseguridad : https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad

gob.mx. (21 de mayo de 2018). *CIDGE.* Obtenido de Artículos: https://www.gob.mx/cidge/articulos/fortalecimiento-de-los-mecanismos-de-ciberseguridad?idiom=es

Islas, O. (21 de Abril de 2017). *Peridico El Universal.* Obtenido de Opinión, Penetracion Mundial de Internet: http://www.eluniversal.com.mx/entrada-de-opinion/columna/octavio-islas/techbit/2017/04/21/penetracion-mundial-de-internet

IWS. (10 de mayo de 2018). *Internet World Stats*. Obtenido de America Stats, México: https://www.internetworldstats.com/central.htm#mx

Knight, B. (27 de 06 de 2017). *DW.* Obtenido de Actualidad/Política: https://p.dw.com/p/2fVYx

Leyva, J. (28 de 04 de 2018). Presunto 'hackeo' al sistema de pagos de Banxico pega a operación. Mexico, México, México.

Morales, A. (22 de enero de 2018). *El Universal, Nación.* Obtenido de Seguridad: http://www.eluniversal.com.mx/nacion/seguridad/propone-senadora-imponer-pena-de-prision-de-15-40-anos-por-ciberterrorismo

RAE. (24 de 05 de 2018). *Real Academia Española.* Obtenido de Diccionario de la Lengua Española Ed. del Tricentenario actualización 20: http://dle.rae.es/?id=98Wdd57

Sanchez Medero, G. (2012). Ciberespacio y el Crimen Organizado. *Revista Enfoques (Santiago)*, 71-87. Obtenido de http://132.248.9.34/hevila/RevistaenfoquesSantiago/2012/vol10/no16/3.pdf

Sarukhán, A. (18 de febrero de 2018). *Revista Letras Libres.* Obtenido de Política: Geopolítica, redes sociales y la elección en México: http://www.letraslibres.com/mexico/revista/geopolitica-redes-sociales-y-la-eleccion-en-mexico

UNDOC. (2013). *El uso de internet con fines Terroristas.* Viena: Naciones Unidas.