Universidad Nacional Autónoma de México

Facultad de Estudios Superiores Aragón

Cambios en la seguridad internacional en el marco de la globalización: el caso de la ciberseguridad y sus desafíos para la Seguridad Nacional de México (2012-2018)

Tesis que para obtener el título de:

Licenciado en Relaciones Internacionales

Presenta:

Jorge Luis Aguirre Ramírez

Asesor de tesis:

Lic. Efrén Martín Badillo Méndez

Ciudad Nezahualcóyotl, Estado de México, 2019

Agradecimientos y dedicatorias

A mi familia:

Primeramente, agradecer a mis padres (Yolanda y Enrique) por todo el apoyo brindado hasta el momento, sin lugar a dudas, ustedes son un valioso soporte en mi vida académica y personal. Les agradezco por ser mi guía, mi primera escuela y mi mejor aprendizaje; este logro es compartido, pues es un trabajo de los tres. Los amo.

A mi abuelita María Luisa, por todo su apoyo y cariño a través de los años, por sus enseñanzas, cuidados y preocupaciones hacia mí. Una dicha el tenerte en la vida. Te amo tanto.

Para todos mis tíos y primos en general, pero particularmente a mi tío Gabriel, por siempre brindarme un buen consejo para abordar la vida, por apoyarme, preocuparse por mí y preguntarme cada vez que me veía sobre este trabajo de investigación.

A mi Root (Alan) por ser mi hermano en esta vida. Por todos estos años de diversión, soporte, alegrías y peleas. Espero que cada día te superes más, eres un orgullo para mí.

A mi familia Aguirre en general, pero particularmente a mi abuelita Victoria y mi abuelito Enrique, por tantas alegrías y apoyo. Los amo tanto.

A mis amigos:

Alan Arturo, por ser mi mejor amigo. Tantas aventuras, experiencias y alegrías, eres parte importante de esta gran etapa, capitán.

Sharon y Julio, mis grandes amigos de la secundaria que han seguido en este recorrido a pesar del transcurso de los años. Les agradezco mucho.

Óscar Farías, por ser el primer gran amigo que tuve al inicio de los estudios universitarios. Tu apoyo, motivación y conocimiento son una guía para mí. Te admiro, te respeto y te guardo gran estima y cariño.

Edgar Melgoza, por ser el mero mero sabor ranchero. Tus reflexiones, sugerencias, regaños y apoyo siempre los llevaré conmigo. Eres muy especial en mi vida. Para ti, con gran admiración y cariño, hermano.

José Atzin, por todas las locuras, experiencias, risas y enojos que compartimos a lo largo de la licenciatura. Valoro mucho tu apoyo incondicional. Con estima y cariño hacia ti, amigo.

Juan Vega, por tantas cosas que aprendo a diario de ti. Tu dedicación, esfuerzo y compañerismo desde que nos hicimos amigos han sido motivo para respetarte, admirarte y guardarte afecto. Sin ti, la universidad no hubiera sido lo mismo, Juancho.

Mario Barragán, por ser una de las personas que me motivó a comprar el periódico y leer más sobre diversos asuntos. Tu amistad es especial para mí por la reciprocidad en tus acciones y por tu gran compañerismo que siempre me has mostrado. Con admiración y estima hacia ti, amigo.

Aldo Longines, por el apoyo que tu amistad siempre me ha brindado en los días buenos y malos. Los momentos de FIFA, risas, conferencias, ajedrez, intercambio de ideas y análisis, nunca faltaron. Con gran aprecio y admiración hacia ti, Herr Longines.

Karen Avalos, por ser una parte importante en esta etapa y en mi vida. Los aprendizajes, discusiones y alegrías contigo hicieron de la etapa universitaria, la mejor. Te agradezco el haber aparecido en mi vida, desde entonces la llenaste de magia, vida, libertad y revolución en todos sus matices. Con gran aprecio y cariño hacia ti, mujer violeta.

Roque Meza, por ser el mero hermano. Tantas cualidades que tienes, te hacen una persona excepcional. El mayor honor que tengo es compartir la mesa redonda con alguien como tú, mi gran compañero de guerra. Harta admiración y respeto hacia ti, querido amigo.

Diana Martínez, por ser la mera mera sabor ranchera. Tu dedicación, esfuerzo y compañerismo me han hecho aprender grandes cosas de ti. Gracias por tu apoyo en los días buenos y malos. Con gran aprecio y cariño hacia ti, Dianilla Vainilla.

Diana Caracheo, por ser la mejor amiga en esta etapa universitaria. Estos años me permitieron conocerte de muchas maneras, haciéndote una persona muy importante en mi vida. Te agradezco nuestras complicidades, chismes, reflexiones, preocupaciones y apoyo, ¡eres una mujer admirable! Para ti, con gran cariño.

Daniela Santos, por siempre ser distraída en todo. Tu perseverancia, esfuerzo y calidez, te hacen una persona única. Con gran cariño y estima hacia ti, Güerita.

Michael Bracamontes, por ser uno de mis mejores amigos. Bastó poco tiempo para considerar tu amistad como una invaluable y especial. Tu esfuerzo, perseverancia, inteligencia y humildad son valores que me inspiran. Con gran aprecio y estima hacia ti, mi gran amigo y compañero de fórmula para 2036.

Lucio Avila, por tu solidaridad, sencillez y apoyo. Tus conocimientos, trabajo, esfuerzo y dedicación me hicieron respetarte y admirarte, pero sobre todo, valorar tu gran amistad. Me ayudaste de diversas maneras en la realización de este trabajo, al enviarme notas, artículos y demás documentos en la materia. Te agradezco tu compañerismo y amistad, con aprecio hacia ti, amigo erreita.

Zyanya Torres, la niña del moño. Llegaste en mi último año de estudios y te convertiste en ese rayo de luz que iluminó de una manera muy bonita mis días finales en la universidad. Tu esfuerzo, valentía, entusiasmo y libertad, me hacen admirarte. Te agradezco tanto el que hayas aparecido en mi vida. Con cariño y estima para ti, futura Licenciada en RR.II. y Nutriología.

Mi sincero agradecimiento para mi mentor, Lic. Efrén Martín Badillo Méndez. Por ser un excelente guía en el desarrollo de este trabajo. Su profundo conocimiento y experiencia enriquecieron mi crecimiento como internacionalista al grado de aspirar a ser como usted. Muy agradecido el que haya aceptado ser mi asesor. Con gran aprecio y respeto para usted, profesor.

A mis sínodos, Maestro Rodolfo Villavicencio, Maestro Abdiel Hernández, Maestro Alejandro Martínez y Maestra Patricia Baranda. Sus recomendaciones, correcciones y puntos de vista hicieron que este trabajo de investigación fuera mejor de lo que un principio establecí. Les agradezco mucho sus aportaciones.

A la UNAM, por abrirme las puertas desde mi estancia en CCH Azcapotzalco y permitirme seguir estudiando en la honorable Facultad de Estudios Superiores Aragón, a la que le debo tanto, pues es un hogar para mí.

CCH Azcapotzalco Aprender a aprender; Aprender a ser, y; Aprender a hacer	FES Aragón/RR.II. Dadme una palanca, un punto de apoyo y moveré al mundo	UNAM Por mi raza hablará el espíritu

Mi país, nuestro país.

¡Hagamos más grande a México!

SIGLAS Y ACRÓNIMOS

AENOR	Asociación Española de Normalización y Certificación
AIC	Agencia de Investigación Criminal
ANR	Agenda Nacional de Riesgos
BANXICO	Banco de México
CCDCOE	Centro de Excelencia de Defensa Cibernética Cooperativa
CERT-MX	Centro Nacional de Respuesta a Incidentes Cibernéticos
CERTS	Equipos de Respuesta ante Emergencias Informáticas
CESI	Comité Especializado en Seguridad de la Información
CESNAV	Centro de Estudios Superiores Navales
CICTE	Comité Interamericano Contra el Terrorismo
CISEN	Centro de Investigación y Seguridad Nacional
COMEXI	Consejo Mexicano de Estudios Internacionales
CNBV	Comisión Nacional Bancaria y de Valores
CONDUSEF	Comisión Nacional para la Protección y Defensa de Usuarios de Servicios Financieros
CRI	Cuarta Revolución Industrial
CSI	Coordinación de Seguridad de la Información
CSIRT	Equipos de Respuesta a Incidentes de Seguridad Informática
CSN	Consejo de Seguridad Nacional
CSR	Complejo de Seguridad Regional
DARPA	Agencia de Proyectos de Investigación Avanzada de Defensa
DDoS	Ataque de Denegación de Servicio
EDN	Estrategia Digital Nacional

EES	Estrategia Europea de Seguridad
ENC	Estrategia Nacional de Ciberseguridad
ENISA	Agencia de Seguridad de las Redes y la Información
ENSI	Estrategia Nacional de Seguridad de la Información
FIRST	Foro de Respuesta a Incidentes y Equipos de Seguridad
GEG	Grupo de Expertos Gubernamentales
IdC	Internet de las Cosas
IMC	Índice Mundial de Ciberseguridad
IP	Protocolo de Internet
IQNET	Red Internacional de Certificación
ITU	Unión Internacional de Telecomunicaciones
MAAGTICSI	Manual Administrativo de Aplicación General en materia de Tecnologías de Información, Comunicaciones y Seguridad de la Información
MUD	Mercado Único Digital
NCE	Nuevo Concepto Estratégico
NCR	Cibercampo Nacional
NIS	Directiva sobre Seguridad de las Redes y la Información
NSA	Agencia de Seguridad Nacional de Estados Unidos
ONG	Organizaciones No Gubernamentales
ONP	Objetivos Nacionales Permanentes
OTAN	Organización del Tratado del Atlántico Norte
PGR	Procuraduría General de la República
PND	Plan Nacional de Desarrollo

RMA	Revolución de los Asuntos Militares
SCADA	Controles de Supervisión y Adquisición de Datos
SEDENA	Secretaría de la Defensa Nacional
SEGOB	Secretaría de Gobernación
SEMAR	Secretaría de Marina
SF	Sistema Financiero
SFC	Sistemas Físico-Cibernéticos
SHCP	Secretaría de Hacienda y Crédito Público
SNM	Seguridad Nacional de México
SPEI	Sistema de Pagos Electrónicos Interbancarios
SPEUA	Sistema de Pagos Electrónicos de Uso Ampliado
SPF	Servicio de Protección Federal
SSM	Secretaría de Seguridad Multidimensional
TIC	Tecnologías de la Información y la Comunicación
UE	Unión Europea
UICOT	Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas
UNAM	Universidad Nacional Autónoma de México
UNICIBER	Unidad de Ciberseguridad
UNODA	Oficina de Asuntos de Desarme de las Naciones Unidas
URSS	Unión de Repúblicas Socialistas Soviéticas
USNORTHCOM	Comando Norte de los Estados Unidos

ÍNDICE

INTRODUCCIÓN

La Cuarta Revolución Industrial ha generado grandes cambios en la vida de las personas, empresas, organizaciones e instituciones de los países. La innovación digital ha dado soporte a los trabajos que desarrolla el ser humano, principalmente, en los sistemas de producción, lo cual ha generado una dependencia con las Tecnologías de la Información y la Comunicación (en adelante, TIC).

En ese sentido, la Globalización es un proceso que ha dinamizado el intercambio de bienes, de servicios y de tecnologías. Por otra parte, se ha incrementado el flujo de datos existente en el ciberespacio, pues es utilizado como un mecanismo para interactuar e intercambiar información con otros sujetos.

Si bien los beneficios que traen consigo el ciberespacio y la globalización son diversos, también existen efectos negativos para los Estados porque deben multiplicar esfuerzos para atender nuevos retos y desafíos. En ese tenor Manuel Castells precisa que «…la capacidad del Estado Nación resulta decididamente debilitada por la globalización de las principales actividades económicas, por la globalización de los medios… la comunicación electrónica, y por la globalización de la delincuencia».[1]

Esto permite que el crimen organizado, grupos delictivos, terroristas, *hackers* y Estados, puedan usar al ciberespacio como un instrumento para llevar a cabo sus intereses. De esta manera, se puede plantear que el espacio virtual es un escenario de múltiples actores.

A raíz de esto, el ciberespacio es considerado como un factor de riesgo por el Foro Económico Mundial, debido a los potenciales peligros que se pueden desarrollar en la interacción con dicho entorno, principalmente por el uso de códigos maliciosos para atacar objetivos generales y particulares, con el propósito de sustraer información a los usuarios. En el año 2017, hubo dos grandes virus que tuvieron alcances globales. Tenemos el caso de *WannaCry*, que afectó a casi 300,000 computadoras en 150 países, y *NotPetya* que causó pérdidas por $300 millones de dólares.[2]

[1] Manuel Castells, *La Era de la Información Económica, Sociedad y Cultura. La sociedad Red,* Alianza, Madrid, 1998, p. 272.

[2] Joe Tidy, "Me odian y me persiguen por destruir virus en internet", *BBC Mundo*, 19 de marzo de 2019, acceso el 27 de abril de 2019 en https://bbc.in/2kD3soF

Por otra parte, el contexto actual perfila al ciberespacio como un nuevo escenario de operaciones militares, el cual puede ser utilizado para mejorar los ataques convencionales de los ejércitos a través del uso de códigos virtuales, dando paso a las llamadas guerras híbridas.[3] Diversos expertos denominan Quinto Dominio de Guerra al ciberespacio,[4] debido a que algunos Estados están desarrollando capacidades ofensivas y defensivas en dicho entorno virtual. Por lo tanto, como indica Gema Sánchez: «…en un mundo tan hiperconectado e hiperinformatizado como el actual, cualquier impacto en el corazón de los *networks* de la información y la tecnología podría generar pérdidas millonarias a cualquier país o institución, por no hablar de las fuertes consecuencias psicológicas que podría ocasionar un ataque de estas características».[5]

Dichas variables pueden alterar la paz y la seguridad internacional, así como la seguridad nacional de los Estados pues, actualmente, muchas de las instituciones gubernamentales e infraestructuras críticas[6] emplean ordenadores para gestionar sus datos y comunicaciones; de modo que, requieren de altos estándares de ciberseguridad para protegerlos. Un ejemplo práctico para entender la importancia de las infraestructuras críticas es el sistema de distribución de aguas, el cual puede utilizar medios electrónicos como medidores de los niveles de presión, almacenamiento y distribución de dicho recurso; un posible error o ataque

[3] Las guerras híbridas pueden ser entendidas como la mezcla de acciones militares convencionales, tales como enviar tropas a un determinado territorio, pero con la utilización de complementos irregulares como el uso de drones, códigos maliciosos o sofisticados en el ciberespacio para afectar dispositivos electrónicos de los rivales. Para efectos de esta investigación se coincide con lo que describe Javier Jordán, se debe ser cuidadoso a la hora de acuñar conceptos, puesto que denominar guerra híbrida conlleva acciones ofensivas entre uno o más sujetos en el escenario internacional; por lo tanto, para efectos prácticos, es mejor utilizar la palabra conflicto en lugar de guerra. Para saber acerca de esto, véase: http://bit.ly/2lNDQp8

[4] Los otros dominios son el espacio terrestre, el marítimo, el aéreo, el ultraterrestre. En Aurelio Tomás, "La seguridad tiene cinco dominios: aire, tierra, mar, espacio y ciberespacio", *PERFIL*, 07 de julio de 2018, acceso el 27 de noviembre de 2018 en: http://bit.ly/2kDTiUM

[5] Gema Sánchez, "Los Estados y la Ciberguerra", *Ministerio de Defensa: Centro Superior de Estudios de la Defensa Nacional*, España, No. 317, 2010, p. 65, http://bit.ly/2lIXC5i

[6] Para propósitos de ésta investigación, se entiende como institución estratégica, toda aquella encargada de proveer servicios esenciales en materia económica, de seguridad, de defensa, de educación y de salud. A su vez, las infraestructuras críticas son las herramientas que utilizan dichas instituciones para su correcto funcionamiento, las cuales pueden ser medios electrónicos como computadoras, sistemas y plataformas digitales que tienen como propósito brindar eficacia, rapidez y seguridad a determinado sector o población. Para complementar lo anterior, es preciso citar la siguiente definición sobre infraestructuras críticas: «es el conjunto de activos tecnológicos indispensables, que interactúan entre sí para brindar servicios vitales a los habitantes de un país». Para saber más, se recomienda revisar la página 108 (que define las IC) y 78 (que aborda el caso de *Stuxnet*) de esta investigación para tener un amplio panorama de las consecuencias y gravedad de atacar infraestructuras críticas. En Arsenio Aguirre, "Ciberseguridad en Infraestructuras Críticas de Información", Tesis de maestría, Universidad de Buenos Aires, 2017, p.7, http://bit.ly/2kFKyxg

cibernético en contra de tal sistema puede entorpecer el correcto suministro de agua hacia ciertos segmentos de la población, ocasionado desabasto y crisis, es por esto que se le denomina infraestructura crítica.

En tal contexto, es necesario replantear el lenguaje utilizado para los asuntos de seguridad, pues los conceptos clásicos de guerra y seguridad se han visto rebasados ante las nuevas amenazas y riesgos tecnológicos. Por estas razones es conveniente considerar las condiciones del nuevo panorama del siglo XXI, para buscar soluciones innovadoras a los problemas de la actualidad.[7]

En ese orden de ideas, Meschoulam agrega: «…estamos no solamente ante una expansión de los métodos para atacar enemigos, sino ante la manifestación de un fenómeno que los internacionalistas discutimos desde hace décadas: el incremento de actores en el sistema internacional».[8] El hecho de que todos puedan ejercer poder en el ciberespacio[9], involucra a diversos actores que desean trascender tanto en lo interno como en lo externo, debido a que el ciberespacio no tiene fronteras. Por ello, es menester del Estado mexicano considerar los riesgos, implicaciones y oportunidades en el desarrollo de estrategias, políticas y leyes sobre ciberseguridad en el corto, mediano y largo plazo, para evitar efectos económicos negativos a causa de ciberdelitos[10], cibercrimen[11], por información hurtada a través del ciberespionaje o ataques directos dirigidos a infraestructuras críticas del país.

[7] Mary Kaldor, *El poder y la fuerza. La seguridad de la población civil en un mundo global*, Tusquets Editores México, México, 2011, p. 27.

[8] Mauricio Meschoulam, "Ciberguerra en 2016: las armas de disrupción masiva", *El Universal*, 24 de octubre de 2016, acceso el 27 de noviembre de 2018 en: http://bit.ly/2lNz4YM

[9] El ciberespacio puede ser entendido como un espacio virtual que está compuesto por redes y medios informáticos en donde se puede crear, modificar, intercambiar, destruir y bloquear información. Para saber más de esto se recomienda ver la página 35 de esta investigación.

[10] Los ciberdelitos son actividades ilegales que se llevan a cabo en el espacio virtual, de modo que sólo basta con tener los conocimientos necesarios en informática y redes digitales para perpetrar actos como el robo de datos personales y financieros, extorsión, robar identidades y realizar acciones de espionaje cibernético. Para saber más acerca de esto, véase: http://bit.ly/2ktmf5X

[11] El cibercrimen consiste en la materialización de cualquier acto que tenga como propósito causar daño en línea, de acuerdo a los distintos intereses que tenga cierto individuo o grupo de personas. En este sentido, Norton by Symantec lo define como: « […] cualquier delito que se realice en línea o que ocurra principalmente en línea. Abarca desde el robo de identidad y otras violaciones de seguridad hasta actividades como la pornografía vengativa, el acoso cibernético, el hostigamiento, el abuso e, incluso, la explotación sexual infantil. Los terroristas cada vez participan más en Internet y trasladan los crímenes más aterradores al espacio cibernético». En "De qué manera distinguir el cibercrimen y protegerse", *Norton by Symantec*, s.f., acceso el 29 de abril de 2019, https://nr.tn/2lHJwkM

Es por ello que, el título de esta investigación se denomina: «Cambios en la seguridad internacional en el marco de la globalización: el caso de la ciberseguridad y sus desafíos para la Seguridad Nacional de México (2012-2018)». Analizar el tema de la seguridad es algo que se realiza de manera común, debido a que es un concepto que debe ser actualizado para afrontar los retos que la situación requiera. En este sentido, se enfatiza el marco de la globalización como un proceso que ha permitido el surgimiento de nuevos actores, diferentes a los entes estatales, que buscan incidir en el sistema internacional para adquirir poder a través del uso de las Tecnologías de la Información y de la Comunicación.

El caso de la ciberseguridad no pasa desapercibido, pues actualmente, se pueden generar severos daños económicos, políticos y sociales, que ponen en riesgo el orden público, tanto nacional como internacional, por la utilización del ciberespacio como una herramienta que permite desarrollar acciones ilícitas en el entorno virtual con impacto en el mundo real. Tan es así, que se pueden paralizar las actividades de un país, o bien, destruir las infraestructuras críticas que tienen componentes digitales, estas pueden ser las que proveen de servicios esenciales a la población o las que son estratégicas en materia de seguridad y defensa. La navegabilidad en la red no tiene límites ni fronteras, de modo que un código malicioso desarrollado en cierta parte del planeta puede causar efectos directos tanto de manera específica, como de manera masiva.

Atacar a través del entorno virtual, pone en riesgo la seguridad del sistema internacional, así como la seguridad nacional de los Estados. Analizar el caso de México es vital, debido a que en la gestión sexenal del ex Presidente Enrique Peña Nieto (2012-2018), se dio un impulso hacia el plano digital. Esto requiere de altos estándares en seguridad cibernética, especialmente, en los ámbitos de la seguridad y defensa nacionales. Es por esto que la seguridad nacional del país, debe estar a la vanguardia de las innovaciones tecnológicas-digitales, particularmente en lo que respecta a la ciberseguridad.

En dicha gestión se buscó incrementar el alcance de las Tecnologías de la Información y la Comunicación, no obstante, parece que se pasó desapercibido elevar los alcances de la ciberseguridad a nivel general. Tan es así que, del año 2017 al 2018, México descendió 35

lugares en el Índice Mundial de Ciberseguridad (IMC).[12] Anteriormente ocupaba la posición número 28, sin embargo en la última medición del año 2018, México se encuentra en el lugar 63. El primer lugar es ocupado por Reino Unido de la Gran Bretaña e Irlanda del Norte, mientras que la posición 175 la tiene Maldivas, la cual es la última de acuerdo al IMC.[13]

Pese que en las últimas fases de dicho sexenio se creó una Estrategia Nacional de Ciberseguridad, no ha sido suficiente para hacer frente a los ataques cibernéticos que sufre el país en el ámbito político, económico y social. Es necesario puntualizar que en México uno de los sectores más vulnerables es el económico-financiero, debido a que es un área clave en la que muchos delincuentes ven una oportunidad de sustraer recursos. Un ejemplo de esto es que las empresas pierden aproximadamente, de manera anual, 24 millones de dólares[14].

Por lo tanto, el objetivo general de la presente investigación es: analizar la situación internacional en lo referente a la ciberseguridad para explicar los desafíos que tiene México en materia de seguridad nacional, teniendo en cuenta que los ciberataques, de distintos tipos, seguirán aumentando a medida que exista más innovación tecnológica digital.

Una vez planteado ese aspecto general, se establecen los siguientes objetivos particulares para ahondar en los propósitos de la investigación, por lo que se pretende:

- Facilitar el entendimiento de los conceptos sobre la globalización, la cuarta revolución industrial, la seguridad nacional e internacional, los complejos de seguridad regional, el ciberespacio y sus derivados.
- Destacar las acciones que han realizado algunas organizaciones internacionales como la Organización de las Naciones Unidas, y otras de carácter regional como la Organización del Tratado del Atlántico Norte (OTAN) y la Organización de los Estados Americanos (OEA), y el caso particular de la Unión Europea (UE) en el ámbito de la ciberseguridad.

[12] Rodrigo Riquelme, "México cae 35 lugares en Índice Global de Ciberseguridad de la ITU", *El Economista*, 06 de mayo de 2019, acceso el 07 de mayo de 2019, http://bit.ly/2ma6VeS
[13] "Global Cybersecurity Index 2018", International Telecommunication Union, 2019, http://bit.ly/2lHoMts
[14] La Razón Online, "Vulnerables a hackeo 6 de cada 10 firmas", *La Razón de México*, 26 de marzo de 2019, acceso el 08 de mayo de 2019, http://bit.ly/2kaVAup

- Describir y analizar los ciberataques en Estonia, Irán y *WannaCry,* para determinar si el ciberespacio debe ser considerado un nuevo dominio de guerra.
- Analizar los impactos económicos, políticos y sociales, causados por el empleo de ataques cibernéticos en México. A su vez, precisar cuáles son las instituciones estratégicas e infraestructuras críticas del país en materia de seguridad, defensa e inteligencia nacional en relación con la ciberseguridad.
- Enfatizar las acciones sobre ciberseguridad del sexenio 2012-2018, tomando como referencia el Plan Nacional de Desarrollo, el Programa para la Seguridad Nacional y los Informes de Gobierno. Con base en ello, determinar los avances de México en la materia para así definir los problemas y desafíos que tiene el Estado mexicano en los asuntos de seguridad nacional en relación con la ciberseguridad.

Las teorías que servirán de soporte para analizar este trabajo son la Teoría de Complejos de Seguridad Regional y la Teoría de Globalización, debido a que el carácter analítico de ambas, permitirá explicar cómo un asunto de seguridad puede cambiar y ser desarrollado de acuerdo a la circunstancia. Ambos enfoques tienen un sustento muy particular, pero en conjunto se complementan y coadyuvan a establecer un análisis más preciso sobre el caso de la ciberseguridad. La primera hace énfasis en los agentes securitizadores, puesto que son actores que pueden expandir la agenda de seguridad. Mientras que, la segunda profundiza en las implicaciones que tiene la globalización como un proceso que ha permitido la expansión de agentes no estatales, al crear nuevos canales de comunicación que les dotan de mayores alcances a nivel local, regional e internacional.

De esta manera, la interrogante general que se pretende responder es: ¿Cuáles son los desafíos para la Seguridad Nacional de México en el contexto de la globalización y la ciberseguridad, teniendo en cuenta los cambios existentes en la seguridad internacional?

A su vez, también es pertinente realizar los siguientes cuestionamientos particulares: ¿Por qué la globalización y la Cuarta Revolución Industrial han generado cambios en la seguridad nacional e internacional? ¿Qué rol tienen las organizaciones regionales e internacionales en la securitización de la ciberseguridad? ¿Por qué debe considerarse el ciberespacio como un factor de riesgo? ¿Cuál es el rol de las instituciones mexicanas encargadas de la seguridad y defensa en el contexto de la ciberseguridad?

Para sustentar los fundamentos de la presente investigación, la hipótesis es la siguiente:

Con la globalización, el sistema internacional ha tenido cambios significativos por el empleo de innovaciones tecnológicas, pues generan diversos alcances que los actores utilizan para ampliar sus intereses, de tal manera que los beneficios aumentan, pero los efectos negativos también. En ese sentido, surgen nuevas amenazas y riesgos que afectan la seguridad de distintas maneras, lo cual ha provocado un debate sobre el aspecto restringido de la seguridad y su expansión hacia una perspectiva multidimensional. El ciberespacio ha modificado el esquema tradicional de la seguridad, puesto que diversos actores lo utilizan como una herramienta que sirve para causar daños y sustraer información de sectores estratégicos; revolucionando, de manera significativa, las estrategias ofensivas y defensivas de los Estados. **Si México no reforma la Ley de Seguridad Nacional del año 2005 para que responda a los retos y desafíos digitales del ciberespacio, y a su vez, no logra constituir una política de Estado que contemple la seguridad nacional y la ciberseguridad como factores de desarrollo permanentes, entonces el país será vulnerable en los diversos sectores que emplean las innovaciones tecnológicas de la Cuarta Revolución Industrial, dando lugar a que se incrementen las deficiencias en dicha materia respecto a otros sujetos y actores en un entorno de competencia globalizado.**

A su vez, se precisan las siguientes cinco hipótesis particulares para cada capítulo. A saber:

1. Si el ciberespacio es empleado para llevar a cabo acciones ilícitas, entonces diversos sujetos y actores podrían utilizar los avances de las Tecnologías de la Información y la Comunicación para favorecer sus intereses.
2. Debido a la inestabilidad en el sistema internacional, las organizaciones regionales e internacionales definen sus agendas de riesgos y amenazas, por lo tanto seguritizan ciertos tópicos, como el de la ciberseguridad.
3. La creación de capacidades ofensivas y defensivas en el ciberespacio permite que se desarrollen armas cibernéticas, por lo que algunos sujetos y actores buscan generar ciberpoder[15] para favorecer sus intereses.

[15] El ciberpoder es definido en el capítulo 3.

4. Si las instituciones de México encargadas de la seguridad y defensa nacionales, logran incursionar en tiempo y forma en las innovaciones de la Cuarta Revolución Industrial, entonces podrían revertir los problemas que padece México por ataques cibernéticos.
5. Si la seguridad nacional es parte del desarrollo de todo Estado, entonces México debe modificar y actualizar sus esquemas tradicionales de seguridad para hacer frente a los riesgos y amenazas que provienen del ciberespacio.

Respecto al orden de los capítulos, el primero aborda el aspecto teórico-conceptual que tiene como propósito definir el marco explicativo en lo referente al proceso de Globalización, la Cuarta Revolución Industrial, la seguridad nacional e internacional, y el ciberespacio y sus derivados. De esta manera, se precisa la diferencia entre una agenda de seguridad restringida (a la que comúnmente denominan tradicional) y una multidimensional como premisa comparativa para determinar la naturaleza de los nuevos riesgos y amenazas en el siglo XXI.

En el segundo capítulo, se hace un estudio de las principales organizaciones internacionales que desarrollan el tema de la ciberseguridad desde un determinado eje de acción. El caso de la ONU es excepcional, debido a la magnitud de sus operaciones y porque es la máxima representante de los Estados en una gran cantidad de temas. En ese sentido, las investigaciones, análisis y resoluciones, adquieren una perspectiva neutral de los tópicos que son abordados a través de sus organismos y agencias especializadas, tal es el caso de la Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA, por sus siglas en inglés) y la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés), que tratan el tema de la ciberseguridad de acuerdo a sus competencias y atribuciones.

También se analizan la Unión Europea, la Organización del Tratado del Atlántico Norte y la Organización de los Estados Americanos para determinar cuál es su enfoque al respecto, y con ello, precisar cuáles han sido sus principales avances en el asunto de la ciberseguridad.

El tercer capítulo tiene como eje de análisis los incidentes en Estonia, las centrifugadoras en Irán, y los problemas ocasionados por *WannaCry*. Dichos sucesos, son ejemplos prácticos que permiten dimensionar los efectos negativos que pueden ocasionar el empleo de ataques cibernéticos. Su estudio sienta las bases para observar qué, cuándo, dónde y cuáles fueron

las principales consecuencias de dichos acontecimientos. Esto explica si el ciberespacio debe ser considerado un nuevo dominio de guerra, o bien, si es necesario categorizarlo como un escenario de conflicto permanente.

En el cuarto capítulo, se enfatizan los principales incidentes cibernéticos que ha tenido México. De esta manera, se describen los daños, los principales problemas y las vulnerabilidades que tiene el Estado mexicano en el ámbito de la seguridad cibernética[16].

Por otra parte, se precisan las instituciones encargadas de atender la problemática en lo referente a ciberseguridad, ciberdefensa y seguridad nacional. En ese tenor, también se hace énfasis en las infraestructuras críticas y el sector financiero, debido a que son las que tienen mayor probabilidad de sufrir ataques cibernéticos, ya que sus peculiaridades los convierten en objetivos de distintos actores.

El último capítulo analiza someramente la situación actual de la Seguridad Nacional de México con el fin de plantear los desafíos que tiene México en relación con la ciberseguridad. A su vez, se considera la Ley de Seguridad Nacional del año 2005 para reforzar y hacer hincapié en los problemas y vulnerabilidades que tiene el Estado mexicano ante la coyuntura digital.

Por otra parte, se aborda el Plan Nacional de Desarrollo del sexenio de Enrique Peña Nieto (2012-2018) para determinar las bases, líneas de acción y estrategias en lo referente a ciberseguridad; además, el estudio complementario del Programa para la Seguridad Nacional (2014-2018) permite definir cuáles fueron los objetivos planteados en el ámbito de la seguridad cibernética. Para contrastar lo que se hizo en la pasada gestión sexenal, se especifican los resultados de los seis informes de gobierno de dicha administración. Además, se especifica que la ciberseguridad es un elemento indispensable para México en el contexto de la Cuarta Revolución Industrial, de modo que si se considera como un eje de desarrollo nacional, a futuro se podrían reducir los riesgos en dicha materia.

La implementación de la Estrategia Nacional de Ciberseguridad es tomada en cuenta en esta investigación debido a que es una base sustancial para el desarrollo y progreso de México en dicha área. En tal sentido, se consideran algunas recomendaciones que emitió la

[16] La seguridad cibernética es entendida como ciberseguridad, puesto que son sinónimos.

OEA hacia México, y con base en ello, se contrasta que, para hacerla funcional, es necesario que su modificación, implementación y desarrollo sea continuo.

Por último, se señala la relevancia de la cooperación internacional como un mecanismo que puede aprovechar México para afrontar los desafíos que se presentan en el entorno digital, y con ello, aplicar soluciones óptimas en lo referente a la ciberseguridad y su relación con la seguridad nacional.

CAPÍTULO 1

LA GLOBALIZACIÓN ECONÓMICA Y LA CUARTA REVOLUCIÓN INDUSTRIAL Y SUS IMPLICACIONES EN LA SEGURIDAD INTERNACIONAL, LA SEGURIDAD NACIONAL Y LA CIBERSEGURIDAD

En la época contemporánea, las dinámicas nacionales e internacionales se encuentran en constante cambio, por lo cual, es necesario generar nuevos aportes que nos ayuden a explicar por qué ocurren dichos acontecimientos a través de la aplicación de teorías.

En el área de las Relaciones Internacionales, un objeto de referencia es la dinámica internacional, la cual se desarrolla a través de la interacción constante entre Estados, no obstante se han establecido nuevos conceptos y teorías dentro de la disciplina para coadyuvar al desarrollo de un sustento que argumente por qué suceden dichos cambios.

El contexto actual se caracteriza por la irrupción de las Tecnologías de la Información y la Comunicación, es por ello que las innovaciones tecnológicas son un factor a considerar porque tienen un carácter global, lo que implica instrumentar argumentos innovadores que dimensionen los nuevos alcances que la Globalización y la Cuarta Revolución Industrial han generado en los Estados-Nación, así como en las Organizaciones Internacionales, ocasionando efectos directos en las agendas de seguridad.

1.1 Teoría de la Globalización

El proceso de globalización ha impactado tanto en las relaciones internacionales, que ha causado en el mundo la necesidad de readaptar conceptos que adquieran nuevas dimensiones para abordar las realidades que la coyuntura exige, generando para ello un estudio y análisis más particular.

Para comenzar, se debe precisar una definición como elemento base de esta teoría, esto con el fin de entender las implicaciones y retos que supone para la seguridad. En dicho sentido, Reyes establece:

> La globalización es una teoría entre cuyos fines se encuentra la interpretación de los eventos que actualmente tienen lugar en los campos de desarrollo, la economía, los escenarios sociales y las influencias culturales y políticas. La globalización es un conjunto de propuestas teóricas que subrayan especialmente dos grandes tendencias: a) los sistemas de comunicación mundial; y b) las condiciones

económicas, especialmente aquellas relacionadas con la movilidad de los recursos financieros y comerciales.[17]

De acuerdo con el trabajo de Held y otros autores, la globalización es concebida como un proceso, o serie de procesos, en el cual, las transformaciones en la organización espacial tienen repercusión en las relaciones y transacciones sociales considerando su alcance, intensidad y velocidad. Dicho espectro tiene una magnitud transcontinental e interregional en las actividades en que se ejerce poder.[18]

Es destacable mencionar las dos tendencias de la primera definición que refieren a los sistemas de comunicación mundial y a lo económico-financiero. En lo que respecta a la segunda definición, se habla de procesos y transformaciones que tienen diversas características que pueden repercutir en el ejercicio del poder.

Los canales de la globalización tienen muchas competencias a nivel internacional, generando diversas variaciones en el cómo se conducen las relaciones entre los actores que son participes en tal escenario. Aunado a ello, cabe mencionar la importancia que tienen las Tecnologías de la Información y la Comunicación (TIC), puesto que como herramientas de comunicación, conectan a los países distantes de manera veloz. Un punto característico de lo que menciona Held es que se destaca la velocidad, el alcance y la intensidad en este proceso.

Dicho de otro modo, la globalización erosiona simbólicamente las fronteras entre los países, por lo que sus interacciones son más dinámicas; principalmente en lo financiero. No obstante, los demás sectores (político, militar, societal, ambiental y diplomático), también comienzan a tener mayor injerencia en el plano internacional e interregional, lo que trae beneficios; pero también conflictos, pues fragmenta y crea roces entre los que buscan incidir en el ejercicio del poder.

En tal sentido, se ha generado una interdependencia intersectorial entre los países, lo que repercute en la manera tradicional en la que se concibe la realidad internacional, para

[17] Giovanni Reyes, "Teoría de la Globalización: Bases fundamentales", *Revista de la Facultad de Ciencias Económicas y Administrativas*, vol. 2, n.° 1, 2001, p. 44, http://bit.ly/2kD58OZ

[18] David Held., *Transformaciones globales. Política, economía y cultura*, Oxford University Press, México, 2002, p. 49. Citado en Ricardo Piana y Juan Cruz, "Globalización, interdependencia compleja y mundialización: la dialéctica entre lo global y lo local", *Razón Crítica*, 3, 2017, p. 157, http://bit.ly/2ma7Agm

enmarcar esta premisa, Keohane y Nye precisan que « […] la naturaleza de la política mundial está cambiando».[19] Tan es así que, el empleo del ciberespacio en el marco de la Cuarta Revolución Industrial (CRI), modifica de manera directa e indirecta los modos de producción y los modelos de seguridad.

La teoría de la globalización, establece que existen efectos que impactan en la naturaleza del sistema internacional, lo que la escuela realista de las Relaciones Internacionales considera anárquico, pues la mayor parte de su análisis está centrado en el Estado y los factores de poder. Sin embargo, el proceso globalizador tiene una injerencia en esto, porque permite que se creen nuevos canales de comunicación para que otros actores adquieran un relativo protagonismo, esto les da acceso, en cierto grado, a ser partícipes en dicho sistema.

La interdependencia, destaca al Estado, a los organismos internacionales y regionales en su dinámica particular como en sus relaciones mutuas. Sin embargo, también inserta a la competencia a actores no estatales como empresas multinacionales, Organizaciones No Gubernamentales (ONG) y, en el ámbito societal, a los individuos.[20]

El proceso de globalización e interdependencia constituyen una transformación de la sociedad internacional, lo que implica la necesidad de introducir nuevos conceptos que sirvan de fundamento para atender los cambios que derivan de dicha transformación. Más aún si se toma en consideración el contexto en donde prima la información.

El flujo de información cobra gran relevancia por la necesidad que tienen los actores de acceder a ella, lo que presupone una nueva fase para el desarrollo de sus políticas, en ese sentido Borja y Castells enfatizan que:

> El planeta es asimétricamente interdependiente y esa interdependencia se articula cotidianamente en tiempo real, a través de las nuevas tecnologías de información y comunicación, en un fenómeno históricamente nuevo que abre de hecho una nueva era de la historia de la humanidad: la era de la información.[21]

[19] Robert Keohane y Joseph Nye, *Poder e interdependencia*, GEL, Buenos Aires, 1988, p. 19. Citado en Piana y Cruz, "Globalización, interdependencia compleja…", p. 162.
[20] Ibíd., p. 163.
[21] Jordi Borja y Manuel Castells, *Local y Global. La gestión de las ciudades en la era de la información*, Taurus, España, 1997, p. 21.

Las Tecnologías de la Información y la Comunicación, trascienden las fronteras de manera casi inmediata, de modo que las innovaciones dinamizan cada vez más ese flujo. Esto representa un factor crítico porque adquiere un sentido transnacional, por lo que el aspecto geográfico se ve rebasado o limitado ante el sentido restringido que predominaba en el pasado siglo.

Para dilucidar el aspecto del transnacionalismo, Ortega y González presentan las tres siguientes premisas:

> Las relaciones transnacionales son interacciones sociales a través de las fronteras no controladas, dirigidas o protagonizadas por los órganos centrales ni de política exterior de Estados nacionales, más bien son protagonizadas por actores que pueden ser individuos, hogares, colectividades y organizaciones con estructuras formales o informales actuando en redes.
>
> Estas relaciones generan espacios sociales transnacionales a partir del intercambio, circulación y flujos de información, personas, bienes materiales e inmateriales, símbolos y representaciones.
>
> Los circuitos transnacionales se forman en espacios sociales transnacionales que conectan dos o más espacios geográficos. Los flujos transnacionales generan impactos en los espacios geográficos conectados.[22]

Derivado de lo transnacional, los nuevos actores pueden ejercer gran influencia política, económica, ideológica y cultural, desde un plano positivo. Aunque también el terrorismo y el crimen organizado pueden tener acceso con relativa facilidad a los canales que derivan del transnacionalismo.[23]

Hay tres elementos que coadyuvan al entendimiento de la globalización y la interdependencia, esto marca una diferencia entre lo local y lo global. Los tres puntos, que destacan Nye y Keohane, son:

- Canales múltiples: refieren a los conductos que posibilitan la comunicación entre las sociedades. En ese sentido, se matiza que las relaciones ya no son únicamente entre Estados, por lo que las políticas locales adquieren un mayor énfasis en el plano global.

[22] Adriana Ortega y Misael Gónzalez, "Transnacionalismo", en *Teorías de Relaciones Internacionales en el siglo XXI,* editado por Jorge Schiavon *et. al.*, Asociación Mexicana de Estudios Internacionales, A.C, México, 2016, p. 459.
[23] Ibíd., p. 458.

- Ausencia de jerarquías: la agenda de los Estados ya no es lineal porque ahora deben atender una gran variedad de temas. Es decir, la agenda adquiere un nivel múltiple de tópicos donde un tema puede ser más prioritario que otro dependiendo de la coyuntura.
- Menor rol de las fuerzas armadas: los conflictos dejan de ser meras confrontaciones entre ejércitos, lo que deriva en la especialización de otros factores para ejercer coerción sobre un adversario.[24]

Nye y Keohane desarrollan «los procesos políticos de la interdependencia compleja», y se desenvuelven en tres niveles más, siendo estos los siguientes:

- Estrategias de vinculación: los Estados buscarán asociarse de acuerdo a sus capacidades e intereses, teniendo en consideración su estatus o jerarquía.[25]
- Establecimiento de la agenda: la ausencia de jerarquías tiene repercusión sobre la definición de qué tema adquiere más importancia que otro. Con ello, la seguridad puede ser la base, pero otro tópico puede adquirir mayor relevancia.
- Relaciones transnacionales y transgubernamentales: las relaciones ya no son llevadas a cabo estrictamente por los Estados, sino que las ciudades y actores no estatales adquieren una relevancia significativa; en ese sentido, se vuelve difícil puntualizar qué es un tema de naturaleza nacional o internacional.[26]

El aspecto global adquiere un rasgo distintivo y está estrechamente relacionado con la interdependencia compleja, pues tiene características similares, otorgándole un fundamento más preciso para explicar los cambios en el sistema internacional derivado del proceso de la globalización y de los efectos que ha ocasionado la Cuarta Revolución Industrial.

Es preciso puntualizar que lo global viene inmerso en un nuevo marco que debe ser definido por poseer características múltiples debido a la influencia que ejerce el proceso globalizador, haciendo alusión a la era de la información, el ciberespacio transforma las relaciones de

[24] Piana y Cruz, "Globalización, interdependencia compleja…", p. 163.
[25] Se explica que los Estados que tienen mayor capacidad militar, tienden a vincularse por motivos de coerción y fuerza, mientras que los que poseen menor potencial en ese rubro, son propensos a cooperar e interactuar mediante la diplomacia en los organismos internacionales.
[26] Piana y Cruz, "Globalización, interdependencia compleja...", p. 164.

poder con la incorporación de nuevos conceptos, actores y procesos que integran un nuevo espacio en el escenario internacional.

1.2 La Cuarta Revolución Industrial

Para comenzar con el análisis, es necesario establecer una definición para tener un marco de referencia de las implicaciones de lo que es una Revolución Industrial. El Diccionario de la Real Academia Española define la palabra Revolución[27] de dos maneras, como «cambio profundo, generalmente violento, en las estructuras políticas y socioeconómicas de una comunidad nacional»; y como «cambio rápido y profundo en cualquier cosa». Para el término Industrial[28] como adjetivo se refiere a, «lo perteneciente o relativo a la industria» y como significado, a toda «persona que vive del ejercicio de una industria o es propietaria de ella».

Landes define la Primera Revolución Industrial como «el complejo de innovaciones tecnológicas que, al sustituir la habilidad humana por la maquinaria y la fuerza humana y animal por energía mecánica, provoca el paso desde la producción artesana a la fabril, dando así lugar al nacimiento de la economía moderna».[29]

Por lo tanto, tenemos como palabras claves, complejo de innovaciones tecnológicas, esto es un elemento característico de las posteriores revoluciones industriales, y es que a partir de la Primera, los Estados-Nación comenzaron a tener una dinámica acelerada hacia la innovación de los procesos de producción.

De acuerdo al sitio web *Salesforce Latinoamérica*, quién cita al Dr. Klaus Schwab (Director Ejecutivo del Foro Económico Mundial), menciona que «una revolución industrial se caracteriza por el surgimiento de nuevas tecnologías y nuevas maneras de percibir el mundo que impulsan un cambio profundo en la economía y la estructura de la sociedad».[30]

En ese sentido, las demás Revoluciones Industriales se caracterizan por cambios en las estructuras de la economía, la sociedad y la política. De acuerdo al mismo portal antes

[27] "Revolución", *Real Academia Española*, s.f., acceso el 10 de septiembre de 2018 en: http://bit.ly/2mb8ol6
[28] "Industrial", *Real Academia Española*, s.f., acceso el 10 de septiembre de 2018 en: http://bit.ly/2kv0H91
[29] Landes, D.S., *Proceso tecnológico y revolución* industrial. Tecnos, Madrid, 1979, p. 15. Citado por Julián Chaves, "Desarrollo Tecnológico en la Primera Revolución Industrial". *Norba. Revista de Historia* N° 17, 2004, p. 96, http://bit.ly/2kD5BAJ
[30] "¿Qué es la Cuarta Revolución Industrial?", *Salesforce Latinoamérica*, acceso el 10 de septiembre de 2018 en: https://sforce.co/2lHp9Em

mencionado, la Segunda Revolución Industrial está caracterizada por el uso de la ciencia y la producción masiva alimentada por la electricidad; la Tercera es fomentada por el uso de la computación y las tecnologías digitales; y finalmente, la Cuarta por la expansión tecnológica intensa. Para entender las complejidades y nuevas realidades de la Cuarta Revolución Industrial (CRI), es preciso conocer el contexto de la Tercera debido a que es la antesala de los desarrollos de la actual.

El marco inicial de la Tercera se desarrolló en la década de los años 1950, en el cual se comenzaron a crear los primeros elementos sobre la microelectrónica, los *mainframes*, y además, se establecieron los primeros debates acerca de la inteligencia artificial; en ese sentido, gran parte de la información tenía su transmisión a través de un canal análogo, pero con un impulso hacia el proceso de digitalización.[31]

CUADRO 1. FUNDAMENTOS DE LAS CUATRO REVOLUCIONES INDUSTRIALES[32]

Primera Revolución Industrial	Segunda Revolución Industrial	Tercera Revolución Industrial	Cuarta Revolución Industrial
•Máquina de vapor •Energía Hidráulica •Mecanización	•Producción en masa •Cadena de montaje •Electricidad	•Automatización •Tecnologías de la Información y la Comunicación (TIC)	•Internet de las Cosas •Nube •Coordinación Digital •Sistemas ciberfísicos •Robótica

Con base en ello, Schwab menciona que la Cuarta Revolución Industrial no debe ser definida por un conjunto de tecnologías emergentes, sino por la transición hacia nuevos sistemas que tienen como base la infraestructura de la revolución digital anterior.[33]

Aquí destaca la premisa hacia el proceso de digitalización, el cual ha tenido gran impacto en la economía, pues una característica esencial de ésta, es el alto componente de información digitalizada. En ese orden de ideas, se debe enfatizar que el mundo ha cambiado a diferencia

[31] Ibíd.
[32] Elaboración propia con datos obtenidos en Vicent Selva, "Revolución Industrial IV", *Economipedia*, s.f., acceso el 11 de septiembre de 2018 en: http://bit.ly/2m3OWqf
[33] Valeria Perasso, "Qué es la Cuarta Revolución Industrial (y por qué debería preocuparnos)", *BBC Mundo*, 12 de octubre de 2016, acceso el 11 de septiembre de 2018 en: https://bbc.in/2kFU4jZ

de hace 10 años, pues hoy en día todo está conectado y tiene una tendencia de seguir digitalizándose.[34]

Uno de los componentes de la CRI, tiene que ver con el «Internet de las Cosas», porque en los años recientes ha tenido un gran auge e impacto en la utilización de los dispositivos electrónicos en relación a las principales actividades que llevan a cabo las personas, de modo que se habla de una interconexión con los instrumentos digitales como un medio para facilitar la vida de los seres humanos.

En ese tenor, es necesario precisar la diferencia entre *Internet* y *Web*. De acuerdo al «Informe Técnico de Cisco» del año 2011, el término *Internet* significa «la capa física o la red compuesta de *switches*, *routers* y otros equipos. Su función principal es transportar información de un punto a otro, de manera veloz, confiable y segura».[35] El término *Web* se refiere a «una capa de aplicaciones que opera sobre la superficie de internet. Su rol principal es proporcionar una interfaz que permite utilizar la información que fluye a través del Internet»[36].

Por tal motivo se debe comprender que el *Internet* de las Cosas (en adelante IdC), se refiere a que la mayor parte de las cosas que utilizamos están conectadas a *Internet*. Un ejemplo de esto es el siguiente:

> […] los automóviles actuales tienen múltiples redes para controlar el funcionamiento del motor, las medidas de seguridad, los sistemas de comunicación y así sucesivamente. De forma similar, los edificios comerciales y residenciales tienen distintos sistemas de control para la calefacción, la ventilación y el aire acondicionado, la telefonía, la seguridad y la iluminación.[37]

La idea de que se pueda controlar todo esto es posible, con el empleo del *Internet* de las Cosas, puesto que el modelo consiste en conectar los dispositivos físicos a partir de una coordinación digital mediante el uso del *Internet*. En ese tenor, un escrito realizado por Telcel en 2014, establece que la hiperconexión tiene como propósito hacer que los dispositivos

[34] Cristina Fonseca, "¿Cómo capacitarnos para la Cuarta Revolución Industrial?", *World Economic Forum*, 16 de enero de 2017, acceso el 11 de septiembre de 2018 en: http://bit.ly/2kDVrzO
[35] Dave Evans, "Internet de las Cosas. Cómo la próxima evolución de Internet lo cambia todo", *CISCO*, 2011, p. 5, http://bit.ly/2kfRRvG
[36] Ibíd.
[37] Ibíd., p. 4.

adquieran la capacidad de comunicarse con otros objetos a través de una dirección de *Internet*.[38]

Por otra parte, también es relevante señalar el impacto del denominado *Big Data* (en español, Datos Masivos), en los demás componentes o procesos de la CRI. El término anterior se refiere a que:[39] «es un conjunto de datos o combinaciones de conjuntos de datos cuyo tamaño (volumen), complejidad (variabilidad) y velocidad de crecimiento (velocidad) dificultan su captura, gestión, procesamiento o análisis mediante tecnologías y herramientas convencionales».

En la coyuntura actual, la importancia del *Big Data* para las empresas, instituciones y gobiernos es fundamental, pues el hecho de que la información sea digitalizada implica que es necesario contar con los componentes necesarios para salvaguardar y procesar toda la información almacenada en datos. Ejemplo de esto, es el gran volumen de información que se genera a partir del uso de dispositivos móviles, redes sociales, envío de archivos multimedia como audios, vídeos o imágenes; además de los equipos industriales que emplean sensores digitales para la generación de datos de alto valor a través de medidores eléctricos.[40]

Además, es oportuno destacar que los campos de información son globales, de modo que la cantidad de datos que circulan por las redes es exponencial. Ante ello, los términos como *gigabyte* (mil millones de *bytes*) o *terabyte* (un billón de *bytes*), comienzan a ser desplazados y a quedar fuera de orden porque el flujo de información es tanto que ahora se requieren expandir las capacidades de almacenamiento.

Los términos que se están adaptando al nuevo contexto son los *petabytes* (mil billones de *bytes*) o *exabytes* (un trillón de *bytes*), los cuales tienen una mayor capacidad de guardar información.[41] Lo más seguro es que en un futuro cercano, dichos términos puedan quedar

[38] Telcel, "Internet de las Cosas", *Forbes México*, 18 de diciembre de 2014, acceso el 11 de septiembre de 2018 en: http://bit.ly/2lNAFxK

[39] "Big Data: ¿En qué consiste? Su importancia, desafíos y gobernabilidad", *PowerData*, s.f., acceso el 11 de septiembre de 2018 en: http://bit.ly/2lIZbQI

[40] Ricardo Barranco, "¿Qué es Big Data?", *IBM developWorks*, 18 de junio de 2018, acceso el 11 de septiembre de 2018 en: https://ibm.co/2kGgzFF

[41] Paolo Gaudiano, "Qué entendemos por «cosas» en el Internet de las cosas", *Fundación de la Innovación Bankiter* , 2011, p. 13, http://bit.ly/2ma96iy

desactualizados, pues la realidad es que la información global genera, de manera creciente, cada vez más datos.

La CRI trae consigo una gran serie de cambios por los componentes de esta revolución tecnológica, siendo el *Internet* de las Cosas, la Robótica, el *Big Data*, la Nube, la Inteligencia Artificial, las más representativas. Es por ello que las sociedades, la economía, la política e incluso el sector militar se encuentran adaptando todo lo anterior a los procesos productivos y de la vida diaria por los beneficios que trae; además, dichos instrumentos se siguen innovando y actualizando. En este sentido, se debe hacer énfasis de que lo anterior se seguirá desarrollando en el futuro próximo, causando que los cambios traigan consigo retos, posibilidades, pero también una serie de riesgos y peligros.

La CRI genera beneficios, pero también efectos negativos, pues estas tecnologías son utilizadas para el desarrollo de la industria militar. Las innovaciones con propósitos bélicos, representan un riesgo para la seguridad internacional, no sólo porque los Estados pueden emplearlas, sino porque incluso otros actores de igual manera tienen acceso a dichas tecnologías y pueden utilizarlas inconvenientemente, incidiendo en la estructura de seguridad del sistema internacional.

1.3 Seguridad Internacional y Seguridad Nacional

El aspecto de la seguridad es uno de los elementos más importantes para los Estados-Nación, pues sirve para definir una serie de objetivos, estrategias y acciones encaminadas a proteger su soberanía ante cualquier posible amenaza o riesgo que pueda presentarse a nivel nacional o internacional.

Para tener un entendimiento sobre esto, es necesario mostrar una definición sobre el concepto de seguridad para después atender el criterio de lo internacional y lo nacional. El Diccionario de la Real Academia Española define ‘seguridad’ como «cualidad de seguro».[42] Aunado a lo anterior, en la disciplina de las Relaciones Internacionales, existen muchos aportes de diferentes escuelas de pensamiento que brindan un panorama amplio sobre los estudios de seguridad, por lo que no hay una definición que sea universal para todos.

[42] “Seguridad”, *Real Academia Española*, s.f., acceso el 11 de septiembre de 2018 en: http://bit.ly/2kD4YXK

Dependerá de las circunstancias, el contexto y el interés nacional del Estado en la elaboración de sus planes de seguridad y defensa.

Por otra parte, la evolución del concepto de seguridad ha sido constante por los diferentes conflictos que han tenido lugar a partir de las dos Grandes Guerras Mundiales, siendo éstos dinámicos en su grado de complejidad e innovación tecnológica.

Thomas Hobbes,[43] establece en su libro «El Leviatán», que las naciones están destinadas a vivir en un estado perpetuo de guerra, por lo que, el razonamiento generado recae en el comportamiento de los hombres. En ese orden de ideas, Kenneth Waltz menciona en «El hombre el Estado y la guerra», que, «los hombres no son guiados por los preceptos de la razón pura, sino por sus pasiones. Los hombres, guiados por la pasión, son arrastrados al conflicto. En lugar de ayudarse mutuamente, se comportan de una manera que es mutuamente destructiva».[44]

Con un argumento similar al anterior, Adler precisa que «el complejo de inferioridad en algunos seres humanos es lo que los conduce a dominar a los demás»[45]. Dicha premisa enmarca el concepto dominación, el cual emplea el componente del ejercicio de poder para someter a otro sujeto. En esa tesitura, Clausewitz destaca que «la guerra es un acto de fuerza para obligar a nuestro enemigo a hacer nuestra voluntad».[46] La imposición de normas, ideologías, creencias y pago de tributos hacia otro grupo organizado a través de instrumentos bélicos, forja la necesidad de incrementar y fortalecer los mecanismos de defensa para contrarrestar las acciones punitivas del adversario. Lo anterior da sustento al denominado *dilema de la seguridad*.

Dicho concepto nos permite explicar que los Estados (como unidad de análisis para el dilema de seguridad), están inmersos en un sistema internacional anárquico, por lo tanto se encuentran en plena desconfianza los unos de los otros. En ese orden de ideas, Terradas explica:

---

[43] Fue un filósofo inglés que nació en el año 1588 y murió en 1679. En "Nació filósofo Thomas Hobbes", *History*, s.f., acceso el 11 de septiembre de 2018 en: http://bit.ly/2ke4JlZ

[44] Kenneth Waltz, *El hombre, el Estado y la guerra. Un análisis teórico*, Centro de Investigación y Docencia Económicas, México, 2013, p. 27.

[45] Carl von Clausewitz, *On War*, Princeton University Press, Nueva Jersey, 1984, p. 75. Citado por Walter Astié y María Rosas, *Las relaciones internacionales en el siglo XXI*, Universidad Nacional Autónoma de México, México, 2017, p. 59.

[46] Ibíd., p. 58

> La condición anárquica del sistema genera incertidumbre, la cual da lugar a la desconfianza, que también provoca un profundo dilema según el cual aquellas personas que toman decisiones en nombre de un estado nunca pueden estar "100% seguros" de si sus cálculos sobre las intenciones futuras de los demás son correctos. Todo ello compele a los estados a desconfiar y a competir (necesariamente) en aras de proveerse seguridad, y prevalecer.[47]

Es por ello que la seguridad para uno, significa inseguridad para otro. En el sistema internacional hay actores antagonistas que potencian y fortalecen su sector militar y armamentista; no obstante, existen otros que en sus agendas e intereses nacionales tienen por hoja de ruta intereses contrarios. Tal escenario permite que algunos Estados tengan que verse obligados a mantenerse alertas, pues otros se encuentran desarrollando armamento que podría ser visto como amenaza a sus intereses.[48]

El dilema de la seguridad es una característica del pensamiento del realismo clásico donde el Estado-Nación es el actor más importante para el estudio y análisis del sistema internacional; derivado de dicha escuela de pensamiento es que se originaron los principales aportes sobre seguridad en el contexto del fin de la Segunda Guerra Mundial y el comienzo de la Guerra Fría.

Las diferencias entre Occidente y Oriente causaron un conflicto que permitió el establecimiento de dos bloques, el socialista bajo el liderazgo de la Unión de Repúblicas Socialistas Soviéticas (U.R.S.S.), y el capitalista bajo la dirección de los Estados Unidos. La rivalidad y competencia por ganar esferas de influencia hizo posible que se desarrollara una carrera armamentista, en la cual hubo un gran progreso tecnológico-militar-industrial; tal escenario convirtió al sistema internacional en un complejo bipolar.

Sin embargo, la culminación de la Guerra Fría propició un cambio en el entorno internacional, pasando de un complejo bipolar a uno multipolar, de tal manera que se modificaron las agendas de desarrollo de los países, y con ello, las estructuras del sistema. En este sentido, el concepto tradicional de la seguridad comenzó a ser planteado desde otros enfoques, sobre todo desde una perspectiva social y con tendencia a tener como objeto de referencia

[47] Nicolás Terradas, "El dilema de seguridad y su importancia para el estudio de las relaciones internacionales", *Revista Letras Internacionales*, n.° 88-3, 2009, acceso el 12 de septiembre de 2018 en: http://bit.ly/2lPckYk

[48] Ángela Arbeláez, "La Noción de Seguridad en Thomas Hobbes", *Revista Facultad de Derecho y Ciencias Políticas*, vol. 39, n.° 110, 2009, p. 109, http://bit.ly/2lPcn6s

a las personas (seguridad humana) y ya no bajo el entendimiento restringido o tradicional del aspecto territorial del Estado.[49]

La globalización y la creciente interdependencia entre la seguridad internacional y la seguridad nacional, hicieron posible una modificación del espectro de la seguridad, generando un debate teórico en dicha materia; a raíz de ello, surgieron tres corrientes de pensamiento: los tradicionalistas, los ampliacionistas y los críticos.[50]

Los tradicionalistas tienen como base el realismo y neorrealismo; los ampliacionistas se basan en la idea de que la agenda de seguridad debe cubrir más temas, además del militar; y finalmente los críticos abordan el latente riesgo que representa la securitización del discurso de acuerdo a los tomadores de decisiones.[51]

El comienzo de la postguerra fría permitió tener un enfoque múltiple de los nuevos retos y amenazas. En lo referente a las amenazas, el proceso de la globalización ha hecho posible que se expandan en diversos sectores, lo que representa un desafío para los Estados, puesto que no pueden combatirlas estrictamente a través del sector militar debido a que los problemas o riesgos no se resolverían, necesariamente, con el empleo de la fuerza.[52]

En lo que respecta al conflicto, lo que diferencia a las nuevas de las viejas amenazas, es el uso de estrategias más sofisticadas, que en sintonía con las nuevas tecnologías y recursos disponibles, pueden causar daños más severos y directos a los Estados, así como a las sociedades.[53]

Complementando la premisa de las amenazas, Cujabante establece:

> Las amenazas no tradicionales, por su parte, representan un peligro difuso, en la medida en la que la fuente de donde provienen es indeterminada, multidimensional,… [por lo que] las amenazas pueden provenir de diferentes temas y [por otra parte es] multidireccional, pues estas… pueden atentar contra la seguridad de actores estatales como no estatales.[54]

[49] Astié y Rosas, *Las relaciones internacionales…*, p. 366.
[50] Ibíd.
[51] Ibíd.
[52] Ibíd., p. 370
[53] Ibíd., p. 372.
[54] Ximena Cujabante, "La seguridad internacional: evolución de un concepto", *Revista de Relaciones Internacionales, Estrategia y Seguridad*, vol. 4 n.° 2, 2009, p. 101, http://bit.ly/2lHqkUi

Las nuevas amenazas, particularmente las que emplean tecnología digital pueden generar repercusiones a nivel global por lo antes referido, y es que actualmente tienen la posibilidad de incidir en la seguridad internacional y sembrar de múltiples maneras, riesgos a la misma, pues tienen dos características a considerar, la multidimensionalidad y lo multidireccional. En un ambiente anárquico y de constantes cambios, los Estados deben procurar mantener el orden público internacional a través de la cooperación y el multilateralismo, pues cualquier anomalía que represente una amenaza o riesgo a la seguridad internacional,[55] puede repercutir en su seguridad nacional.

Seguridad Nacional

Muñoz menciona que «la seguridad de un Estado se construye y adapta de manera circunstancial, modificándose de acuerdo a las necesidades de cada país y adaptándose a los contextos de historia, cultura y sociedad».[56] Esto debe responder primeramente a las capacidades del Estado para el desarrollo de su seguridad nacional.

Por otra parte, Piñeyro define la seguridad nacional de la siguiente manera:

> Una situación en la que la mayoría de los sectores y clases sociales de la nación tiene garantizadas sus necesidades culturales y materiales vitales mediante las decisiones del gobierno nacional en turno y de las acciones del conjunto de las instituciones del Estado, es decir, una situación de relativa seguridad frente a amenazas o retos internos o externos, reales o potenciales, que atenten contra la reproducción de la nación y del Estado.[57]

Otro aporte lo realiza J. Cintra, quién define la seguridad nacional como:

> […] la garantía que, en grado variable, es proporcionada a la nación, principalmente por el Estado, a través de acciones políticas, económicas, psicosociales y militares para que una vez superados los antagonismos y presiones se pueda conquistar y mantener los Objetivos Nacionales Permanentes.[58]

[55] Para efectos de esta investigación, defino a la seguridad internacional como el conjunto de medidas que aplican los Estados de manera unilateral, bilateral o multilateral para asegurar su supervivencia y promover sus intereses en el escenario internacional. Dichas medidas pueden ser diplomáticas, coercitivas, o de cooperación, con el fin de superar antagonismos, así como hacer frente a los distintos tipos de riesgos y amenazas que puedan vulnerar su actuar.

[56] Alejandra Muñoz, "La corrupción como amenaza a la seguridad nacional tras la transición democrática en México", tesis de licenciatura, Universidad de las Américas Puebla, 2005, p. 8.

[57] José Luis Piñeyro, *La seguridad nacional en México. Debate actual*, Universidad Autónoma Metropolitana-Azcapotzalco México, 2005, p. 21.

[58] Cintra, José T., *Seguridad Nacional, Poder Nacional y Desarrollo*, CISEN, México, 1997. Citado por Edmundo Salas, "Reflexiones en torno a la Seguridad Nacional y la Seguridad Interior", *Revista de Administración Pública*, vol. L, n.°1, 2015, p. 294, http://bit.ly/2lKeDMB

Cintra y Piñeyro tienen un enfoque distinto, no obstante, ambas definiciones pueden ser complementarias al encontrar puntos similares. Piñeyro resalta el aspecto de mantener un punto de seguridad para hacer frente a las amenazas o riesgos, ya sean a nivel interno o externo para que el Estado logre sus intereses. En un sentido similar, Cintra infiere que el Estado debe garantizar la seguridad a través de la implementación de diversas estrategias en distintos ámbitos para concretar los intereses estatales, en este caso los Objetivos Nacionales Permanentes.[59]

Es preciso puntualizar que a nivel internacional el concepto de seguridad nacional trae consigo una serie de interpretaciones muy distintas entre sí, por lo que no hay una definición unificada del concepto. De manera similar, es parecida la situación que existe con la seguridad internacional, pues muchos académicos, militares, políticos y estrategas conciben realidades distintas; no obstante, el factor común consiste en asegurar su supervivencia y promover sus intereses. Por lo tanto, el concepto de seguridad nacional puede ser distinto entre Estados debido a que cada uno establece sus mecanismos de acción, así como sus términos, para dar fundamento a sus leyes, instituciones y sectores estratégicos para la preservación de su soberanía y la defensa de sus intereses.

La seguridad nacional tiene que tener un carácter sólido y actualizado para que sirva de sustento en el combate a las amenazas y riesgos, manteniendo de este modo los intereses del Estado en el corto, mediano y largo plazo. Para lograrlo, es necesario establecer un marco jurídico-operativo que sea acorde a la coyuntura, considerando también las capacidades materiales e inmateriales para la consecución de las metas nacionales; por lo tanto, las aspiraciones nacionales[60] son los objetivos que un Estado desea conseguir tanto al interior como al exterior, sin embargo es prioritario establecer el cómo hacerlo para que se definan las metas o los objetivos nacionales.[61]

De esta manera, se infiere que se deben definir cuáles son los riesgos y amenazas a la seguridad nacional para poder establecer las bases de una serie de estrategias y planes,

[59] Ibíd.

[60] Mercado Jarrín describe que «cuando los intereses nacionales se integran a la conciencia nacional, se convierten en aspiraciones nacionales… los intereses vitales se relacionan con las necesidades relevantes de una nación». En Piñeyro, *La seguridad nacional en México…*, p. 29.

[61] Marco Bandala, "Reconceptualización de la Seguridad Nacional: una aproximación para México", *ININVESTAM*, documento de análisis DA. 24/18, 2018, p. 4, http://bit.ly/2kfn1TU

para que sea posible la defensa efectiva del Estado. De no hacerlo, sería difícil crear mecanismos de respuesta si no se tienen en cuenta las adversidades que pueden causar inestabilidad en las acciones de la Nación. Al considerar esto, es preciso tener un óptimo sistema de inteligencia que ayude a identificar potenciales peligros.

Astié y Rosas precisan la diferencia entre amenaza, riesgo y vulnerabilidad. Respecto a la primera, consideran que es todo flagelo que compromete la supervivencia del Estado. El riesgo se define en términos de posibilidad o probabilidad de que un efecto negativo pueda acontecer; y la vulnerabilidad es la exposición que un Estado puede tener ante un riesgo.[62]

Asimismo, las vulnerabilidades se pueden controlar al reducir los efectos del posible peligro, ya sea «mediante la mitigación, predicción, alerta y preparación»; o bien, «fortaleciendo la capacidad para resistir y hacer frente a los peligros».[63]

En un sentido similar, De Miguel considera que existen 3 niveles de riesgos, a saber:

> […] primer nivel, aquellos factores que son una amenaza a la seguridad nacional tanto por la probabilidad que se materialice, como por las consecuencias que tendría para la seguridad nacional; en un segundo nivel, los que bien por su probabilidad,… por su impacto, pueden ser un peligro, y por tanto van a requerir un especial seguimiento y la adopción de medidas preventivas; y en un tercer nivel, se considerarían aquellos riesgos que por su probabilidad o impacto no requieren medidas más allá que las relacionadas con la alerta temprana y la preparación de algunos planes de contingencia.[64]

Es por ello que las estrategias en materia de seguridad tienen que ser formuladas tomando como punto de partida la totalidad de riesgos, o al menos los que tengan mayor probabilidad de afectar la seguridad nacional.[65]

Al considerar los riesgos y amenazas, se pueden garantizar mejores respuestas de acción. En esa tesitura, De Miguel agrega:

> […] las estrategias de seguridad nacional, requieren de un amplio conocimiento de la realidad internacional, así como del contexto social del propio Estado; sus objetivos y líneas de acción deben ser definidos con un enfoque integral, de amplio espectro, y con un marcado carácter proactivo, considerando tanto los riesgos potenciales como las posibles amenazas a enfrentar. Las respuestas a

[62] Astié y Rosas, *Las relaciones internacionales…*, p. 369.
[63] Ibíd.
[64] Jesús de Miguel, "Construyendo una estrategia de seguridad nacional para México", *ININVESTAM,* documento de Análisis, DA. 25/16, 2016, p. 4, http://bit.ly/2k6nZ4C
[65] Ibíd.

> aquellas amenazas que atenten a los intereses nacionales, quedarían así integradas como medidas de defensa nacional, lo que se podría denominar "estrategias de defensa", o más apropiadamente "planes de defensa", formando parte de las propias estrategias de seguridad nacional.[66]

De Miguel toca un punto relevante, cuando habla de tener un amplio conocimiento de la realidad internacional, y es que si no se tiene la visión de los acontecimientos externos, sería difícil establecer una seguridad nacional acorde a los desafíos que el contexto exige. De modo que es de suma importancia conocer los posibles peligros tanto al interior como al exterior.

En ese sentido Curzio enfatiza que existen connotaciones políticas e ideológicas que no siempre fomentan el debate y discusión sobre formular un replanteamiento al concepto de seguridad nacional, en donde al menos deben considerarse cuatro factores («el final de la Guerra Fría; la transición política hacia la democracia; la relativización del concepto de soberanía en un mundo globalizado; y la crisis generada por el terrorismo internacional»)[67] para formular nuevos fundamentos que posibiliten el establecimiento de un nuevo concepto de seguridad nacional.[68]

Con base a lo anterior, es correcto el hecho de que en ocasiones las agendas de los Estados tienen una hoja de ruta diferente, ya sea por los intereses o las capacidades con las que cuenten, de modo que es complejo tratar el tema de la seguridad de manera lineal. En el pasado siglo era relativamente más sencillo focalizarla, debido a que los eventos que se suscitaban en esos momentos por motivo de las guerras de alta intensidad; tal escenario era un condicionante directo, puesto que propiciaban la formulación de políticas nacionales encaminadas a preservar la seguridad y soberanía del Estado desde un enfoque meramente territorial.

Después de la Guerra Fría se han diversificado los desafíos para los Estados. El hecho que marcó un hito fue el 11 de septiembre de 2001, con los ataques a las Torres Gemelas en los Estados Unidos; esto provocó redimensionar y replantear nuevamente el concepto de la seguridad nacional e internacional, caracterizando al terrorismo como un punto crítico dentro

[66] Ibíd., p. 5.
[67] Leonardo Curzio, *La seguridad nacional de México y la relación con Estados Unidos*, Universidad Nacional Autónoma de México, México, 2007, p. 81.
[68] Ibíd.

de las agendas de los países. Por lo tanto, los riesgos y amenazas adquirieron efectos múltiples en sectores que antes no se hubieran pensado.

Con base en ello, Muñoz señala que los Estados se encuentran en una nueva fase de interconexión, por lo cual la economía internacional cada vez se expande y se integran más los países; esto crea un vínculo y una relación diferente a la del siglo XX.[69]

En tal sentido, también menciona que el establecimiento de corporaciones, bancos transnacionales y las nuevas tecnologías crean un marco más complejo de relaciones que tienden a modificar las fuentes de poder,[70] lo que fragmenta las acciones del Estado para preservar la seguridad de manera tradicional. El dinamismo existente ha provocado que la interacción entre Naciones sea más intensa, de modo que la teoría sobre seguridad nacional también requiere que se modifiquen los conceptos tradicionales para generar nuevos significados, tomando en cuenta los asuntos militares, hay rubros que deben ser replanteados.

De tal manera, Taylor precisa que:

> […] la seguridad nacional no sólo es proteger a las personas y al territorio de una invasión física, sino que también representa la protección de los intereses políticos y económicos, que si se pierden, amenazan los valores fundamentales del Estado.[71]

El problema que se vive en cuanto a los debates e implementación de una estrategia de seguridad nacional acorde a las dinámicas del siglo XXI, es que hay una amplia discusión de qué debe ser entendido por seguridad nacional. Algunos teóricos establecen que debe existir una re conceptualización del concepto para adaptarlo a las nuevas realidades, puesto que ya no debe estar restringido meramente a los asuntos de las fuerzas armadas debido a que existen problemas que no pueden ser resueltos con la coerción, tales como el cambio climático, la pobreza, los conflictos económicos e incluso la ciberseguridad.

Los aportes que ha realizado la Escuela de Copenhague, permiten visualizar la seguridad desde otros enfoques, dando énfasis al concepto de seguridad ampliada como una

[69] Muñoz, "La corrupción como amenaza…", p. 23.
[70] Ibíd., p. 16.
[71] Amos Jordan y William Taylor, *American National Security, Policy and Process*, Hopkins University Press, London, 1984, p. 11. Citado en Ibíd. p. 15.

herramienta coadyuvante en la re conceptualización sobre las ideas tradicionales de la seguridad nacional. Base fundamental de esto es la teoría de securitización, que se refiere al binomio "seguridad/protección" como un factor crítico para realizar cambios en el marco del proceso globalizador.

Al abordar el concepto múltiple de la seguridad, De Miguel expresa que:

> […] al hablar de seguridad ampliada nos referimos no sólo a la existencia de nuevos riesgos y amenazas, sino a la necesidad de abordar la seguridad en otros ámbitos, lo que requiere la aplicación de diferentes recursos e instrumentos con un enfoque integral.[72]

Además, es importante considerar que el asunto de la seguridad adquiere un nuevo sentido en el siglo XXI, pues converge con el proceso globalizador y la Cuarta Revolución Industrial, adjudicando nuevos cambios a realizar a fin de tener un concepto más enriquecido sobre la seguridad nacional. Sin eliminar el concepto tradicional de los asuntos militares o dejarlo fuera de contexto, es pertinente interrelacionarlos con el propósito de establecer una visión integradora, lo que posiblemente, supondría la creación de un nuevo paradigma.

De ahí el surgimiento de la Teoría de Complejos de Seguridad Regional, que explica de manera más detallada la relevancia de adaptar la seguridad hacia un plano más reflexivo e integrador, con el propósito de ampliar los objetos referentes en los estudios sobre la seguridad.

1.4 Teoría de Complejos de Seguridad Regional

El espectro de la seguridad comenzó a ser estudiado gradualmente a través de una perspectiva regional casi al término de la Guerra Fría, de modo que se volvió necesario establecer nuevos métodos de investigación sobre los estudios de seguridad para generar marcos de referencia sobre nuevos riesgos y amenazas.

La Teoría de Complejos de Seguridad Regional comenzó a ser desarrollada por Barry Buzan en su libro *People, States and Fear* en el año 1983, que después relanzó en una segunda edición a la que denominó *People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era*, en el año de 1991. Por lo tanto, se puede inferir que éstos dos trabajos fueron los pioneros para la teorización de los Complejos de Seguridad porque

[72] Jesús de Miguel, "Unas reflexiones sobre la seguridad internacional en el siglo XXI", *ININVESTAM*, Documento de Análisis, DA. 06/16, 2016, p. 21, http://bit.ly/2lHLjX2

posteriormente, junto con Ole Weaver y Jaap de Wilde, desarrolló la investigación denominada *Security: A New Framework for Analysis* en el año de 1998, en el cual introducen el término de securitización.

El carácter regional que provee esta teoría es fundamental, porque enmarca una estructura y un análisis particular que permite entender el factor de la seguridad, estableciendo para ello, un objeto referente para su estudio.

Para entender lo anterior, es necesario definir qué es un Complejo de Seguridad Regional (en adelante CSR), Buzan lo denomina como:

> […] un grupo de Estados cuyas principales preocupaciones de seguridad los vinculan entre sí, tan precisamente como para que sus seguridades nacionales no puedan ser consideradas aparte las unas de las de otras.[73]

Posteriormente, con la colaboración y aportes de Weaver, se establece una definición más precisa:

> […] conjuntos de unidades cuyos mayores procesos de securitización y desecuritización, o ambos, están tan entrelazados que sus asuntos de seguridad no pueden analizarse o ser resueltos de manera separada.[74]

Ambas definiciones son complementarias porque la primera es la base, mientras que la segunda se adapta al incorporar el concepto de securitización. En ese tenor, Otálvaro trata de enlazar lo anterior estableciendo la siguiente definición:

> Un perímetro compuesto por diferentes unidades que están intensamente relacionadas en términos de seguridad, al punto de que las dinámicas internas de seguridad de cada una de ellas no podrán ser entendidas ni analizadas por separado sin tener en cuenta a las demás.[75]

Con base en lo anterior, se deben tomar en consideración las palabras «unidades relacionadas en términos de seguridad», debido a que éstas son las que designan qué procesos conducen a la securitización o desecuritización.

---

[73] Barry Buzan, *People, States & Fear, an Agenda for International Security Studies in the Post-Cold War Era*, Harvester Wheatsheaf, London, 1991, p. 190. Traducción propia.

[74] Barry Buzan y Ole Weaver, *Regions and Powers. The Structure of International Security*, Cambridge University Press, New York, 2004, p. 44. Traducción propia.

[75] Andrés Otálvaro, "La seguridad internacional a la luz de las estructuras dinámicas regionales: una propuesta teórica de complejos de seguridad regional", *Desafíos*, 2004, p. 224, http://bit.ly/2lOTf8F

Por tanto, se debe identificar y analizar qué dinámica provoca securitizar algún tópico,[76] tomando en consideración que los riesgos y amenazas tienen un sentido más amplio. Tal escenario obliga a establecer el criterio del tema o circunstancia que se desea impulsar en el desarrollo de la agenda de seguridad de un Estado.

Buzan y Weaver consideran que los asuntos militares no pueden dar solución a todos los problemas, por lo que establecen cinco principales sectores que deben estar presentes en la concepción de una seguridad ampliada, superando de esta manera, el sentido restringido o tradicional de la seguridad. En ese orden de ideas, dichos sectores son: el societal, económico, ambiental, político y militar.[77] Para los propósitos de esta investigación, se propone la ciberseguridad como un nuevo sector referente en los estudios de seguridad, puesto que sus alcances y dimensiones tienen relación con la seguridad nacional e internacional.

CUADRO 2. MULTIDIMENSIONALIDAD DE LA SEGURIDAD POR SECTORES[78]

Sector	Objeto referente	Supervivencia
Societal	Nación	Identidad
Político/Militar	Estado	Soberanía
Económico	Empresas	Evitar crisis
Medioambiental	Naturaleza	Sostenibilidad

Demurtas expresa que «el marco de análisis de la securitización permite expandir la agenda de seguridad hacia un número de sectores más amplio que los de la agenda tradicional».[79] Para ampliar la agenda de seguridad y hacerla multidimensional, también debe considerarse una dirección multisectorial para delinear los propósitos de los actores o agentes

[76] El término securitizar se refiere a cuando un problema pasa a formar parte de manera formal en la agenda de seguridad de un gobierno, justificando la existencia de una potencial amenaza, lo que posibilita el desarrollo y análisis del objeto particular.
[77] Buzan y Weaver, *Regions and Powers…*, pp. 1-10 y 49-193. Citado por Otálvaro, "La seguridad internacional…", p. 228.
[78] Cuadro sustraído en Gabriel Orozco, "El aporte de la Escuela de Copenhague a los estudios de seguridad", Revista Fuerzas Armadas y Sociedad, n.° 1, 2006, p. 149, http://bit.ly/2lKeUz7
[79] Alessandro Demurtas "El complejo europeo de seguridad regional entre 2001 y 2011 a las amenazas del terrorismo islamista y de las armas de destrucción masiva", tesis doctoral, Universitat Autònoma de Barcelona, 2014, p. 39, http://bit.ly/2kDWjo4

securitizadores con sus respectivos objetos de referencia, de modo que pueden ser distintos entre sí, pero también complementarios.[80]

Aunado a lo anterior, los CSR se ven afectados por las constantes interacciones entre los distintos actores y su diversa naturaleza con los procesos subsecuentes de la globalización, lo que diversifica y complica la definición de las agendas de seguridad.[81]

Demurtas establece que el CSR es un patrón de interdependencia lógico del sistema internacional anárquico, por lo que está compuesto a través de una serie de relaciones intersectoriales. De este modo, precisa que:

> Cada sector se rige por relaciones peculiares que permiten distinguirlo de los demás: el sector militar se sustenta en la coerción; el sector político lo hace en la autoridad y la legitimidad; el sector económico se basa en el comercio, la producción y los intercambios; el sector societal se rige sobre las identidades colectivas y, por último, el sector ambiental se apoya en las relaciones entre la actividad humana y los ecosistemas.[82]

Con base en el aspecto regional, Otálvaro menciona que Buzan y Weaver establecen 4 ámbitos de análisis que son el global, regional, interregional y el local o estatal. Para diferenciarlos, a su vez, es pertinente determinar tres tipos de poderes: las superpotencias, las grandes potencias (que operan a una escala global) y las potencias regionales.

El mejor ejemplo de superpotencia lo representa Estados Unidos, por la gran influencia y poderío que ostenta. Se trata del único país que ha propagado universalmente sus valores; además, en el aspecto militar, tiene diversificado su arsenal bélico, diseminado en diversas flotas establecidas en zonas estratégicas, así como bases en diversos Estados.

Todo esto le proporciona un posicionamiento geopolítico internacional único, permitiéndole instrumentar los fundamentos para poner a discusión un tema de seguridad y posicionarlo en la agenda como un asunto crítico que debe ser securitizado, tal y como lo hizo con el terrorismo, que actualmente es considerado como una amenaza y riesgo para la seguridad nacional e internacional.

[80] Buzan y Weaver, *Regions and Powers…*, p. 196.
[81] Otálvaro, "La seguridad internacional…", p. 230.
[82] Alessandro Demurtas "El complejo europeo de seguridad…", p. 43.

Las grandes potencias tienen un importante desarrollo militar y económico, pero no rivalizan con las superpotencias. Esto les permite tener injerencia en diversas regiones del mundo, y con ello, establecer cierta influencia, aunque no para tener un liderazgo mundial en la construcción e imposición de la agenda de seguridad. Ejemplos de éstos son Rusia, China, Francia y Reino Unido, debido principalmente a sus recursos militares y económicos, a los que debe agregarse el aspecto histórico, que en conjunto, les permitiría llegar a convertirse en superpotencia e incidir en dicha agenda.

Por último, se encuentran las potencias regionales, las cuáles no tienen un nivel similar o equiparable a las superpotencias o grandes potencias. En este sentido, no tienen gran presencia global, pero sí regional, por lo que tienen un relativo poder para influir en el desarrollo de la agenda de seguridad con un alcance limitado. Ejemplos de este ámbito son México y Brasil, los cuales participan activamente para asumir un liderazgo en la región latinoamericana. Las condiciones económicas, políticas, sociales y militares, le permitirían a México establecer un determinado asunto como un problema de seguridad. Tal es el caso de la ciberseguridad, puesto que su impacto podría influir en la agenda de desarrollo de otros Estados de manera regional.

Para entender lo anterior, Demurtas precisa un marco operativo para definir la relación de un CSR con base a las amenazas, se basa en las siguientes cuatro preguntas:[83]

1. Una situación que deba ser considerada como un asunto de seguridad por su binomio de riesgo-amenaza. La pregunta para esta investigación sería, ¿la ciberseguridad ha sido securitizada con éxito por algún actor?
2. Si la respuesta es afirmativa, hay que trazar las relaciones e interconexiones con las demás unidades del sistema: ¿existen consecuencias para la seguridad de los demás actores y para otros asuntos relativos a la seguridad?
3. ¿Qué respuesta dan los otros actores del sistema?
4. En último lugar, hay que recopilar las interrelaciones entre las unidades del sistema como si fueran un grupo coherente de preocupaciones sobre la seguridad, evidenciando las interrelaciones y determinando si se confirma la existencia del CSR.

[83] Ibíd., p. 51.

Para que el proceso de securitización de la ciberseguridad se lleve a cabo, se tienen que considerar las siguientes tres unidades de análisis:[84]

1. Objeto referente: sujeto u objeto cuya supervivencia está bajo una amenaza real o percibida.
2. Actor securitizante: el que formula el discurso sobre la seguridad, siendo normalmente la élite política, la burocracia, el gobierno, los *lobbies* y los grupos de presión.
3. Los medios de comunicación.[85]

Aunado a lo descrito por Dermutas, J. Verdes explica que « […] desde una lectura política, al ampliar la noción de seguridad también se acrecentaría con ello el campo de actuación de los órganos del estado en esa materia (ejército, policía, etc.)».[86] En este sentido, es necesario el desarrollo de la ciberseguridad en distintas instituciones gubernamentales por la información de carácter restringido o sensible, que salvaguardan en los dispositivos electrónicos. Por otra parte, el sector privado, a la par que el gobierno, están instrumentando las innovaciones tecnológicas a los procesos de gestión y producción industrial. Esto requiere desarrollar programas, estrategias y políticas que den sustento a las entidades encargadas de proteger y defender el interés nacional, pero desde el ámbito cibernético.

La importancia de esta teoría para los estudios de la seguridad es relevante porque nos permite establecer un análisis más preciso sobre el objeto de referencia (en este caso, el de la ciberseguridad), las agendas de desarrollo y el aspecto de la securitización a nivel global, pero también regional. El aspecto crítico y actualizado sobre la seguridad y la regionalización proporcionan un marco en el que se puede visualizar la necesidad de protegerse desde un enfoque sectorial por la fuerte interdependencia que hay entre los mismos.

El siglo XXI trae consigo una serie de reflexiones y retos que implican necesariamente abordar dicha temática desde un enfoque multidimensional debido a que el marco de la globalización, en conjunto con el fenómeno de la Cuarta Revolución Industrial, también tiene

[84] Ibíd., p. 56.
[85] Demurtas enfatiza que el rol de la prensa nacional es clave para politizar una amenaza hacia la seguridad, ayudando al objeto referente en la percepción o descripción de la amenaza.
[86] Francisco J. Verdes-Montenegro, "Securitización: agendas de investigación abiertas para el estudio de la seguridad", *Relaciones Internacionales*, n.° 29, 2015, p. 114, http://bit.ly/2kfndm6

un carácter de múltiples dimensiones, en donde el desarrollo de estrategias y tácticas defensivas, se desarrolla en el ámbito virtual.

1.5 Ciberseguridad/ciberataque/ciberespionaje/ciberguerra

El término ciberespacio tiene una gran cantidad de definiciones, algunas muy sencillas y otras más complejas, esto depende del medio, institución o individuo que le otorgue un significado de acuerdo a la visión y hoja de ruta que se tenga. La Real Academia Española lo define como un «ámbito artificial creado por medios informáticos».[87]

De acuerdo a la terminología que se encuentra en el sitio del Centro Cooperativo de Excelencia de la Ciberdefensa de la OTAN, el ciberespacio es definido como «el entorno formado por componentes físicos y no físicos, caracterizados por el uso de computadoras y espectro electromagnético, para almacenar, modificar e intercambiar datos utilizando redes informáticas».[88]

Definir qué es el ciberespacio es de gran relevancia, porque es la base para entender los demás términos que derivan de éste, puesto que existen diversos procesos que se desarrollan en ese espacio virtual. Por ello, el ciberespacio es un lugar no tangible que está compuesto por herramientas e instrumentos de informática que permiten la interacción, almacenamiento e intercambio de información con diversos ordenadores o dispositivos a través de redes informáticas.

El progreso e innovación tecnológica que han desarrollado los Estados impacta en la mayor parte de los sectores, porque configura los procesos de gestión, así como las infraestructuras que emplean sistemas informáticos, haciendo posible que algunos resulten más críticos que otros por el tipo de función que tienen para un determinado sector. En este sentido, la mayoría de los países, empresas, instituciones e individuos utilizan ordenadores en donde almacenan una gran cantidad de información; esto supone una gran ventaja en el plano físico porque se reduce espacio y se configura en modo de datos; no obstante, también puede repercutir gravemente en el ámbito de la seguridad informática porque los ordenadores pueden ser vulnerados, hurtados y destruidos.

[87] "Ciberespacio", *Real Academia Española*, s.f., acceso el 16 de septiembre de 2018 en: http://bit.ly/2ma0OXV
[88] "Cyber Definitions", *NATO Cooperative Cyber Defence Centre of Excellence*, s.f., acceso el 16 de septiembre de 2018 en: http://bit.ly/2lPcZsM

Las sociedades se están transformando en sociedades de la información y la comunicación, por lo que integran a su vida diaria el uso de las tecnologías para el desarrollo de sus actividades. Dicha integración también puede ejercer una gran dependencia, porque, en años recientes la mayor parte de los objetos que las personas utilizan, tienen un componente tecnológico digital que permite la interconexión.

En esa tesitura, la Unión Internacional de Telecomunicaciones (ITU) destaca:

> La interconexión extensiva de sistemas, la interdependencia de las infraestructuras, el aumento de la dependencia de las tecnologías digitales, las amenazas y los riesgos, exigen dotar a los individuos, las organizaciones y los Estados de medidas, procedimientos y herramientas que permitan mejorar la gestión de los riesgos tecnológicos y de la información. Los retos del dominio de los riesgos tecnológicos son propios del siglo XXI y exigen un planteamiento global a nivel internacional y su integración en el proceso de la seguridad de los países en desarrollo.[89]

Este elemento representa riesgos que deben ser atendidos por los Estados porque estos son los responsables de proveer seguridad, ante lo cual, deben procurar instrumentar una serie de estrategias en seguridad cibernética que estén a la par de la innovación tecnológica-digital, con el fin de evitar el hurto de información, así como la destrucción de infraestructuras críticas.

En este sentido, la ciberseguridad es definida por la Unión Internacional de Telecomunicaciones en la *Resolución* 181 como:

> […] el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.[90]

[89] "Guía de ciberseguridad para los países en desarrollo", *Unión Internacional de Telecomunicaciones*, 2007, p. 6, http://bit.ly/2lKfq01

[90] "Decisiones destacadas en Guadalajara", *Unión Internacional de Telecomunicaciones*, noviembre de 2010, acceso el 16 de septiembre de 2018 en: http://bit.ly/2kFUVkH

La anterior definición sobre ciberseguridad es una de las más completas, no sólo porque la Unión Internacional de Telecomunicaciones la provea, sino porque engloba un conjunto de elementos, los cuales, si logramos identificarlos, encontramos al menos dos relevantes. El primero se basa en cuestiones técnicas encargadas de brindar seguridad, tales como planes de contingencia, protocolos de acción, políticas y lineamientos a seguir. El segundo podemos catalogarlo como procesos operativos que tienen como propósito proteger la información en los dispositivos electrónicos, como pueden ser la instalación de antivirus, conexiones seguras, entre otros.

Por otra parte, el documento *Perspectiva de ciberseguridad en México* elaborado por el Consejo Mexicano de Estudios Internacionales (COMEXI), en colaboración con McKinsey&Company, definen ciberseguridad como «el conjunto de acciones tomadas por organizaciones e individuos para mitigar los riesgos que enfrentan en el ciberespacio, con el propósito de disminuir la probabilidad de sufrir un ciberataque».[91]

Ambas definiciones centran su análisis en un conjunto de acciones, herramientas o políticas que tienen como propósito atenuar un posible riesgo con el fin de evitar la materialización de un ataque (ciberataque, ciberespionaje, etc). En ese sentido, la definición de la ITU tiene un alcance mayor porque engloba un enfoque de seguridad destinado a salvaguardar la información de los grupos y personas que llevan a cabo el intercambio de datos con el empleo de las redes y canales de comunicación digitales, a través de dispositivos interconectados.

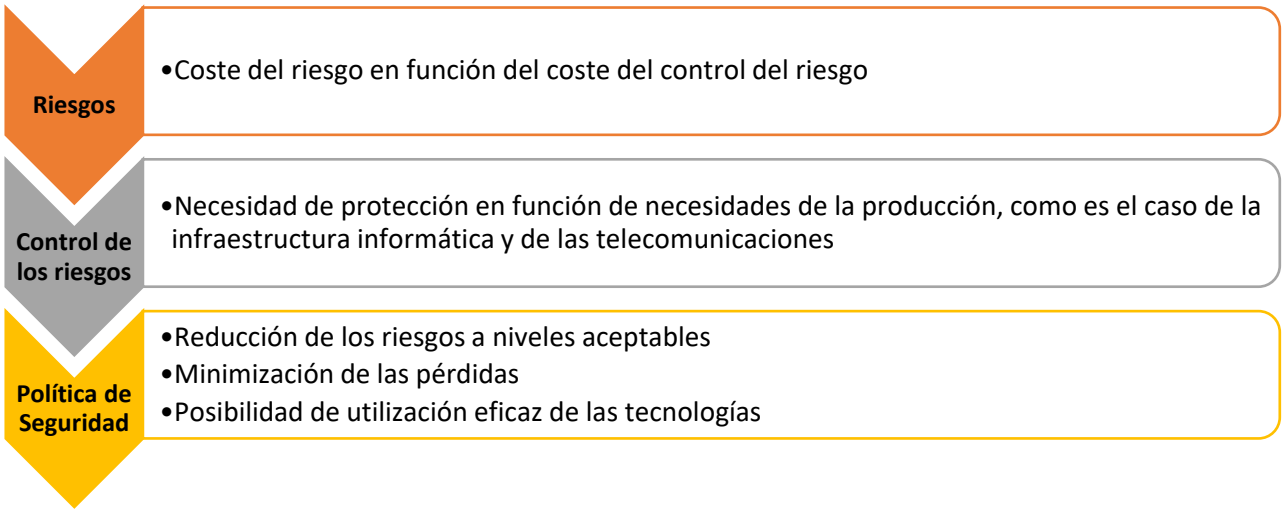
Si tomamos en cuenta las anteriores definiciones, podemos precisar una muy sencilla que sea entendible y clara. La ciberseguridad es la aplicación de un conjunto de procesos técnicos y operativos que buscan minimizar los riesgos en el ciberespacio con el fin de evitar el robo de datos y/o destrucción de los dispositivos, de manera que se garantice una navegación segura en las redes informáticas.

La ITU establece que el objetivo de la ciberseguridad consiste en salvaguardar la información con el fin de reducir la probabilidad de que una amenaza pueda llegar a tener un efecto

[91] Rafael Fernández (coord.), "Perspectiva de ciberseguridad en México", *McKinsey&Company y COMEXI*, Documento colaborativo, 2018, p. 21, http://bit.ly/2kfSZPW

directo en la operatividad y funcionamiento de las empresas, instituciones u organizaciones.[92]

CUADRO 3. CONTROL DE RIESGOS. DEFINICIÓN DE UNA POLÍTICA DE SEGURIDAD[93]



Los riesgos cibernéticos adquieren una mayor intensidad conforme se desarrolla más innovación tecnológica, puesto que sin las condiciones adecuadas en infraestructura, especialización, políticas y legislación en el ámbito informático, los Estados pueden llegar a padecer ciberataques, llevados a cabo por diversos actores con motivos e intereses diferentes.

Ante tal escenario es primordial definir qué es un ciberataque para analizar y dimensionar la importancia de tener una ciberseguridad fuerte, sólida y resiliente porque a nivel internacional, padecer ataques cibernéticos causa daños directos no sólo a empresas e individuos, sino que existen ataques que tienen como objetivo particular un Estado o las instituciones que lo componen.

El término ciberataque es definido por Martínez como «un ataque de ordenador a ordenador que afecta, inhabilita, destruye o toma el control de un sistema informático, o que daña o roba información que dicho sistema contiene».[94]

[92] "Guía de ciberseguridad para…", p. 8.
[93] Elaboración propia con datos obtenidos de "Guía de ciberseguridad para los países en desarrollo", UIT, edición 2007, http://bit.ly/2lKfq01
[94] Clara Martínez, "El uso de ciberataques como herramienta de relaciones internacionales por parte de actores estatales: los casos de Estados Unidos y Rusia", trabajo de fin de grado, Universidad Pontificia Comillas ICAI-ICADE, 2015, p. 9, http://bit.ly/2m3Q6C7

A su vez, la COMEXI y McKinsey&Company refieren que:

> […] es un intento no autorizado por la vía digital de acceder a un sistema de control, dispositivo electrónico y/o red informática, con el propósito de sabotear su funcionamiento, extraer información y recursos, o extorsionar a usuarios y organizaciones.[95]

Las dos definiciones llevan implícito vulnerar un dispositivo, que puede ser un ordenador, un móvil o una infraestructura que emplee un sistema informático. Además, el motivo puede ser la destrucción, el cual implica acabar con el funcionamiento del sistema informático para que sea inaccesible o ya no pueda ser utilizado. Otra intención, puede ser el hurto de información, en donde se infiere que la misma puede ser de carácter personal o sensible, tomando en consideración si se trata del sector financiero, político, militar o diplomático.

Por lo tanto, se habla de que existen dos categorías de ciberataques de acuerdo al impacto que generen; el primero de ellos se refiere a un punto personal-individual en el cual sólo afecta a una persona u organización. El segundo, se basa en lo sistémico, vulnerando un sistema completo que tiene impacto en diversos individuos, organizaciones o instituciones.[96]

Otro aspecto que debe tomarse en cuenta, es la particularidad del ataque, es decir, si es un ataque con un determinado objetivo (ataque dirigido), o bien, que tiene un impacto general y no se basa sobre un objetivo específico (ataque no dirigido). El primero, busca vulnerar la infraestructura, el sistema o los procesos operativos de un determinado objeto; mientras que el segundo es similar al primero en lo que busca; pero la diferencia es que su meta es indeterminada, así que puede perjudicar a un múltiple grupo de personas y entidades.[97] En este sentido, resulta relevante señalar que ambos tienen como propósito causar daño, independientemente de su objetivo.

De acuerdo con Sánchez, todo ataque hacia una red de ordenadores o sistemas informáticos suele seguir las siguientes etapas:

- Descubrimiento y exploración del sistema informático;
- Búsqueda de vulnerabilidades;
- Explotación de las vulnerabilidades;

[95] Fernández (coord.), "Perspectiva de ciberseguridad…", p. 16.
[96] Ibíd.
[97] Ibíd.

- Modificación de programas y ficheros para dejar instaladas puertas traseras, y creación de nuevas cuentas con privilegios administrativos que faciliten el posterior acceso del atacante al sistema; y
- Eliminación de las pruebas que puedan revelar el ataque, incluso, se pueden llegar a modificar las vulnerabilidades descubiertas del sistema.[98]

CUADRO 4. CARACTERÍSTICAS DE LOS CIBERATAQUES.[99]

Bajo coste	•La mayor parte de las herramientas utilizadas por los atacantes pueden obtenerse de manera gratuita o a un coste muy reducido.
Ubicuidad y fácil ejecución	•La ubicación y ejecución de los ataques es independiente de la localización de los agresores, no siendo imprescindible, en muchos casos, grandes conocimientos técnicos.
Efectividad e impacto	•El ataque puede tener o no tener una buena metodología, por lo que depende de su grado de sofistificación. Si no hay una política de ciberseguridad, recursos y capacidades necesarias, el impacto puede ser fuerte.
Reducido riesgo para el atacante	•La facilidad de ocultación hace que sea difícil identificaral autor que lleve a cabo el ciberataque.

En lo que respecta al ciberespionaje, puede entrar en la categoría de ciberataque porque tiene como propósito infiltrarse en la red o sistema informático de un usuario u organización, con el fin de sustraer información; no obstante, tiene características propias que lo diferencian de un ataque cibernético ordinario, puesto que su función no consiste en atacar y destruir, sino que busca sustraer y espiar en los datos de un determinado objetivo.

Los individuos y grupos con habilidades de reconocimiento, atención y sofisticación pueden aprovechar las vulnerabilidades de los sistemas informático, por lo que pueden adentrarse en lo más profundo de los ordenadores y dispositivos electrónicos con el fin de vigilar y si es posible, sustraer los datos más importantes en el sector público o privado, pues hay que

[98] Gema Sánchez, "El ciberespionaje", *DERECOM*, N.° 13, 2013, p. 116, http://bit.ly/2ke5DPp
[99] Elaboración propia con datos tomados de "Estrategia de ciberseguridad nacional", Gobierno de España. Presidencia del Gobierno, 2013, p. 10, http://bit.ly/2m3Qvo7

tener en cuenta que, el objetivo del espionaje cibernético consiste en obtener información crítica o sensible para la elaboración de inteligencia estratégica.[100]

A diferencia del espionaje tradicional, que tiene como propósito vigilar y analizar las actividades de los Estados, organismos e individuos con el objeto de obtener un beneficio que les provea de ventajas sobre quien se está ejerciendo; pero para obtener esa información personal, industrial, política o económica que sea vital para el Estado, éste utilizaría acciones ilegales como espiar o robar dicha información. En tal sentido, las acciones de ciberespionaje vulneran los sistemas informáticos con el fin de espiar y sustraer datos sin que el usuario conceda, de manera legal, la otorgación de los mismos.

En esa tesitura, Arreola menciona tres niveles para la generación de inteligencia:

> Los individuos obtienen datos de su experiencia propia y de agentes investigadores.
> Las empresas tienen grupos de analistas e investigadores de mercado.
> Los Estados cuentan con un organismo o dependencia gubernamental encargado de recopilar todo tipo de información que se convierta en inteligencia.[101]

Arreola, en el último nivel, precisa que los Estados cuentan con un organismo que recopila información para que ésta sea transformada en inteligencia, el punto crítico es saber qué herramientas e instrumentos se pueden utilizar para obtener información que sea beneficiosa para sus propósitos e intereses, pues podrían ser mecanismos ilegales; el desarrollo y empleo de nuevas tecnologías como *softwares* pueden ser un arma potencial para la realización de ciberespionaje sofisticado, el cual puede considerarse más efectivo que el espionaje tradicional.

Por otra parte, lo que se denomina ciberguerra es algo que sigue en constante debate por parte de académicos, expertos y analistas sobre las posibles repercusiones que pudiera

[100] La formulación de inteligencia estratégica consiste en articular un conjunto de información de una o de distintas áreas para que ésta sea procesada y se convierta en conocimiento especializado sobre algún tema en particular. Tradicionalmente, dicho término está ligado a cuestiones que involucran acciones de estrategia y defensa debido a que es necesario poseer conocimientos previos sobre un eventual riesgo o amenaza. En tal sentido, la información obtenida a través de cualquier medio es procesada y organizada a modo de que los tomadores de decisiones tengan las opciones más óptimas en cuanto a la resolución y actuación sobre algún tópico, por lo tanto la inteligencia estratégica es la obtención, articulación y organización de la información a fin de generar conocimiento especializado. Para saber más sobre esto, véase Joao Aguirre, "Inteligencia estratégica: un sistema para gestionar la innovación", *Universidad ICESI*, Estudios Gerenciales, Vol. 31, 2015, http://bit.ly/2lOU2GF

[101] Adolfo Arreola, *Ciberespionaje: la puerta al mundo virtual de los estados e individuos: una revisión de los programas de espionaje digital de Estados Unidos*, Siglo XXI Editores, México, 2015, p. 23.

llegar a tener, o sobre la eventual precipitación de nombrarle guerra cibernética. El punto medular se centra en que no todos los Estados cuentan con la capacidad tecnológica (en términos de infraestructura digital), necesaria para realizar ataques o contrataques en el ciberespacio, a diferencia de los componentes del sector militar tradicional.

En esa tesitura, se infiere que la ciberguerra es una fase que, a largo plazo puede llegar a suceder porque los Estados están desarrollando tecnología, *softwares* y capacidades computacionales para hacer frente a las amenazas que algunos países u otros actores internacionales podrían llevar a cabo.

Sánchez define la ciberguerra como:

> […] una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio, o simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física, sino un ataque informático.[102]

De acuerdo a su definición, la ciberguerra es muy parecida a una guerra tradicional, la diferencia es que se desarrolla en un entorno virtual. Por otra parte, los códigos pueden ser considerados como armas cibernéticas que tienen por meta destruir ciertos objetivos estratégicos. El objeto clave de una potencial guerra cibernética[103], supondría la destrucción de infraestructuras críticas y medios de comunicación que tengan como sistemas operacionales el elemento informático.

El ciberespacio ha tenido un amplio avance a partir del inicio del segundo milenio poniendo de relieve una amplia gama de estudios, investigaciones y desarrollo de capacidades, por lo que se identifica como instrumento innovador que es empleado por diversos Estados y actores internacionales para promover sus intereses a través de la coerción digital. Es por ello que uno de los retos del siglo XXI en lo que respecta al uso del ciberespacio, consistirá

[102] Sánchez, "Los Estados y la Ciberguerra", p. 64

[103] Otra definición que abarca justa y precisamente la ciberguerra es la siguiente: «… es un área dentro de las agencias militares de los países que tiene como objetivo encontrar las vulnerabilidades técnicas de los sistemas o redes informáticas del enemigo para penetrarlas y atacarlas, tanto así como para extraer datos e información sensible. En este caso el ciberespacio es el campo de batalla y las armas son programas o aplicaciones informáticas». En Gustavo Sain, "¿Qué es la ciberguerra?", *Revista Pensamiento Penal*, s.f., acceso el 04 de mayo de 2019, http://bit.ly/2kFBdFL

en detectar, anticipar y neutralizar las ciberamenazas[104]; no obstante, para lograrlo se requiere de altos estándares de ciberseguridad e inteligencia para hacer frente a posibles antagonismos en las redes informáticas.

Es preciso mencionar que se han comenzado a establecer políticas dentro de las agendas de desarrollo de Estados como Rusia, China y Estados Unidos; pero también en organizaciones internacionales como la ONU y regionales como la Organización del Tratado del Atlántico Norte e incluso en los bloques de integración como la Unión Europea.

[104] A diferencia de una amenaza en el entorno físico, la ciberamenaza tiene como característica que su desarrollo se materializa en el espacio cibernético, es decir, en el ciberespacio. Por lo tanto, el ciberentorno, aunque es considerado un espacio intangible, puede tener impactos directos en el mundo real, en lo físico. Una definición de ciberamenaza sería la siguiente: «aquellas actividades realizadas en el ciberespacio, que tienen por objeto la utilización de la información que circula por el mismo, para la comisión de distintos delitos mediante su utilización, manipulación, control o sustracción». En Joaquín Ruiz, "Ciberamenazas: ¿el terrorismo del futuro?", *Instituto Español de Estudios Estratégicos,* Documento de Opinión, 19 de agosto de 2016, acceso el 05 de mayo de 2019, http://bit.ly/2kaclFV

CAPÍTULO 2

LA INSTITUCIONALIDAD DE LA CIBERSEGURIDAD A NIVEL REGIONAL E INTERNACIONAL

Para entender la dinámica internacional en el tema de la ciberseguridad, es importante analizar las acciones, políticas, comunicados, estrategias y resoluciones que han implementado las organizaciones internacionales para hacer frente a las necesidades que dicho tema suscita.

Las principales organizaciones u organismos que atienden el tópico, están conformadas por Estados, por lo tanto, es posible identificar quiénes son los que están trabajando, investigando y elaborando, dentro de sus agendas o programas de desarrollo, el factor de la ciberseguridad.

Además, es preciso señalar que cada entidad trata de manera diferente el tema, pues le dan un enfoque distinto que, puede ser desarrollado por un interés económico, militar, social o político.

2.1 Grupo de Expertos Gubernamentales de Naciones Unidas sobre ciberseguridad

La Organización de las Naciones Unidas (ONU),[105]está conformada por 193 Estados miembros y cuenta con 6 principales órganos,[106] que dan sustento a las labores de gestión y administración de diversos temas. De tal manera, los representantes de los países pueden emitir y expresar sus opiniones a través de recomendaciones para abordar un tópico en cuestión.

La ONU tiene por objetivo el mantenimiento de la paz y la seguridad internacionales, por tal motivo ha creado diversas agencias y oficinas especializadas, que tratan y desarrollan temas con un enfoque social, económico, jurídico, ambiental, entre otros. Dichos asuntos tienen una perspectiva global, pues de no ser atendidos, pueden causar repercusiones negativas en la sociedad internacional.

[105] Las Naciones Unidas se crearon el 24 de octubre de 1945, después, la mayoría de los 51 Estados signatarios del documento fundacional, ratificaron la Carta de la ONU para su entrada en vigor en 1946.

[106] Asamblea General, Consejo de Seguridad, Consejo Económico Social, Consejo de Administración Fiduciaria, Corte Internacional de Justicia y la Secretaría General.

Las Naciones Unidas crearon en el año de 1998, el Departamento de Asuntos de Desarme. Posteriormente, en el año 2007, su denominación cambió a Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA, por sus siglas en inglés).[107]

La UNODA se encarga del desarme nuclear y la no proliferación. Además, fortalece los mecanismos para que se logre el objetivo principal de reducir las cantidades existentes de los diferentes tipos de armamento, que pueden ser, de destrucción masiva o convencional.[108]

Respecto a las armas de destrucción masiva, se considera al armamento nuclear, biológico y químico; mientras que el arsenal convencional, se basa en minas terrestres y armas ligeras, y son las que suelen utilizarse comúnmente. Por otra parte, también toma en cuenta el aspecto de la seguridad de la información como asunto que puede afectar la estabilidad del sistema internacional, debido a su constante innovación en el marco de las Tecnologías de la Información y la Comunicación (TIC).

Los estudios en materia de seguridad de la información, se incorporaron en el año de 1998, debido a que la Federación Rusa presentó un proyecto de resolución que fue aprobado sin someterse a votación. La resolución está clasificada como A/RES/53/70, y lleva por título, «Los avances de la informatización y las telecomunicaciones en el contexto de la seguridad internacional». Los argumentos que determinaron su aprobación derivan de los estudios desarrollados por la Primera Comisión (A/53/576).[109] Dicha resolución destaca los efectos negativos que puede ocasionar, a la seguridad internacional, el uso indebido de las redes de telecomunicaciones y la informatización. Con base en ello, exhortó a los Estados a que realizaran estudios y diagnósticos sobre su situación en materia de seguridad cibernética.

De acuerdo con la UNODA, el primer informe que presentó el Secretario General, recopila las observaciones y recomendaciones realizadas por Cuba, Grecia, México, Panamá, Qatar, Reino Unido de la Gran Bretaña e Irlanda del Norte y Ucrania. Dicho informe fue expuesto como A/65/154, el 20 de julio del año 2010.[110] Lo referido por México, se divide en tres segmentos. Primero, plantea una evaluación general de los problemas de la seguridad de la

[107] "Introducción", *UNODA*, s.f., acceso el 17 de septiembre de 2018 en: http://bit.ly/2kfTycw
[108] Ibíd.
[109] "Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional", *Naciones Unidas. Asamblea General*, A/RES/53/70, acceso el 17 de septiembre de 2018 en: http://bit.ly/2kad1uX
[110] "Informe del Secretario General", *Naciones Unidas. Asamblea General*, A/65/154, acceso el 17 de septiembre de 2018 en: http://bit.ly/2lJ1KCk

información; lo segundo, sobre medidas que se adoptan a nivel nacional para fortalecerla en dicho rubro; y finalmente, sugiere acciones que la comunidad internacional podría implementar para robustecer los esquemas en ese plano a escala mundial.[111]

A partir del año 2010 hasta el 2015, se tienen informes presentados por el Secretario General, a saber:

- 2010 — A/65/154
- 2011 — A/66/152 and A/66/152/Add.1
- 2012 — A/67/167
- 2013 — A/68/156 and A/68/156/Add.1
- 2014 — A/69/112 and A/69/112/Add.1
- 2015 — A/70/172.[112]

A los 10 días de que el Secretario General presentó el informe anual, el 30 de julio de 2010, el Grupo de Expertos Gubernamentales (GEG) presentó su primer estudio A/65/201, denominado «Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional*».*

El informe del GEG, destaca lo siguiente:

> Las amenazas reales y potenciales en la esfera de la seguridad de la información constituyen algunos de los problemas más graves del siglo XXI. Las amenazas derivan de una amplia gama de fuentes y se manifiestan como actividades desestabilizadoras dirigidas por igual contra particulares, empresas, elementos de la infraestructura nacional y gobiernos. Sus efectos entrañan considerables riesgos para la seguridad pública, la seguridad de las naciones y la estabilidad de la comunidad internacional en su conjunto.[113]

Aunado al informe anterior, se establece que las tecnologías son una herramienta que las personas pueden utilizar de doble manera; para el progreso y beneficio de las sociedades, o para ocasionar daños y favorecer intereses particulares.[114] En ese orden de ideas, el

[111] Para conocer lo descrito por México, véase el anexo al final de esta investigación.
[112] "Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional", *UNODA*, acceso el 17 de septiembre de 2018 en: http://bit.ly/2lHrHSW
[113] "Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional", *Naciones Unidas. Asamblea General*, A/65/201, acceso el 18 de septiembre de 2018 en: http://bit.ly/2mbXrzT
[114] Ibíd.

desarrollo negativo de las TIC, puede ocasionar repercusiones directas en la seguridad nacional e internacional.

Derivado del primer estudio del GEG, en el año 2011, la Asamblea General aprobó la resolución A/RES/66/24, en la que se solicitaba al grupo de expertos, el seguimiento y desarrollo del tema para determinar los riesgos y amenazas al orden público. Además, algunos puntos de la resolución exhortan a los Estados a seguir haciendo diagnósticos a nivel nacional para contribuir, en forma de recomendaciones, al informe anual del Secretario General.[115]

El informe bienal 2013-2014 del GEG, fue publicado como documento A/68/98, y en él, se precisa que las normas del Derecho Internacional Público pueden ser aplicables al marco de la seguridad de la información, pues la problemática ocurre en el territorio de los Estados.

En tal sentido, establece:

> […] el derecho internacional, y en particular la Carta de las Naciones Unidas, son aplicables y esenciales para mantener la paz y la estabilidad y para promover un entorno abierto, seguro, pacífico y accesible para las tecnologías de la información y las comunicaciones… también… la soberanía del Estado y las normas y los principios internacionales que emanan de ella son aplicables a la realización de actividades relacionadas con las tecnologías de la información y las comunicaciones por parte de los Estados y a su jurisdicción sobre la infraestructura de tecnologías de la información y las comunicaciones dentro de su territorio; los Estados deben cumplir sus obligaciones internacionales en relación con los hechos internacionalmente ilícitos que se les puedan imputar.[116]

Lo anterior, describe la responsabilidad de los Estados respecto a su soberanía y jurisdicción, por lo que, si ocurren incidentes cibernéticos que afecten a otros países, el Estado donde se suscitó el problema, debe hacerse responsable de las implicaciones del mal uso de las TIC.

En ese tenor, si un virus informático altamente especializado se creó en cierto país y perjudicó a otras Naciones, entonces, se le pueden imputar los agravios por los efectos negativos del código malicioso; no obstante, se debe tener en cuenta la característica del

[115] "Resolución aprobada por la Asamblea General el 2 de diciembre de 2011", *Naciones Unidas. Asamblea General*, A/RES/66/24, acceso el 18 de septiembre de 2018 en: http://bit.ly/2kb0PtY

[116] "Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional", *Naciones Unidas. Asamblea General*, A/68/98, acceso el 18 de septiembre de 2018 en: http://bit.ly/2ktACXW

anonimato en el ciberespacio, pues es bien sabido que resulta difícil rastrear el origen de la elaboración y propagación sobre cierto tipo de virus informático.

Por otra parte, en la sección tercera denominada «Recomendaciones sobre normas, reglas y principios de conducta estatal responsable», se precisa lo siguiente:

> Los Estados deben cumplir sus obligaciones internacionales en lo que respecta a los hechos internacionalmente ilícitos que se les puedan atribuir. Los Estados no deben valerse de agentes que cometan esos hechos por cuenta de ellos. Los Estados deben asegurarse de que su territorio no sea utilizado por agentes no estatales para hacer un uso ilícito de las tecnologías de la información y las comunicaciones.[117]

Lo anterior destaca dos puntos clave: el Estado debe cumplir con su compromiso internacional en caso de ser responsable, y también debe mantener el orden público en el ámbito de las TIC. Por lo tanto, si se asegura esto, es posible reducir el riesgo de que se materialicen ciberataques por parte de agentes no estatales.

Posteriormente, el informe bienal del GEG 2014-2015, fue publicado como documento A/70/174, en el cual se toman en cuenta los aportes de los anteriores estudios para fortalecer el tópico en cuestión. Cabe destacar que, a diferencia de los informes anteriores, se agrega, como nueva sección, la aplicación del derecho internacional al uso de las TIC.[118]

En la sección, «Amenazas reales y potenciales», se abordan seis puntos que contextualizan y exponen los posibles riesgos que pueden materializarse por el uso negativo de las TIC. Sin embargo, para propósitos de esta investigación se enfatizan cuatro amenazas que el informe menciona, a saber:

> Varios Estados están desarrollando capacidad en materia de TIC con fines militares y aumentando las probabilidades de que los futuros conflictos entre Estados entrañen el uso de esas tecnologías;
> Entre los ataques más perjudiciales en los que se utilizan las TIC se encuentran los dirigidos contra la infraestructura fundamental y los sistemas de información conexos de un Estado;
> La utilización de las TIC con fines de terrorismo, más allá del reclutamiento, la financiación, la capacitación y la incitación, e incluso la comisión de atentados terroristas contra las TIC o

[117] Ibíd.

[118] El informe está compuesto de la siguiente manera: 1) Introducción; 2) Amenazas reales y potenciales; 3) Normas, reglas y principios de comportamiento responsable de los Estados; 4) Medidas de fomento de confianza; 5) Cooperación y asistencia internacionales para promover la seguridad y la creación de capacidad en la esfera de las TIC; 6) Aplicación del derecho internacional al uso de las TIC; 7) Conclusiones y recomendaciones para la labor futura.

> infraestructuras dependientes de estas tecnologías, es una posibilidad creciente que, si no se aborda, podría amenazar la paz y la seguridad internacionales;
> Las diferencias en los niveles de capacidad que tienen los Estados en la esfera de la seguridad de las TIC pueden aumentar la vulnerabilidad en un mundo interconectado.[119]

Por otra parte, en la sección titulada «Medidas de Fomento de la confianza», se hace mención de crear canales de comunicación que permitan la cooperación, para hacer más eficiente el intercambio de información técnica-institucional. Para afrontar los riesgos existentes por las vulnerabilidades que se encuentran en el ciberespacio, especialmente, de los que trascienden fronteras, el informe destaca:

> El desarrollo de mecanismos y procesos de consulta bilateral, subregional, regional y multilateral sobre la protección de infraestructuras fundamentales sustentadas en las TIC;
> La elaboración en los planos bilateral, subregional, regional y multilateral de mecanismos técnicos, jurídicos y diplomáticos para hacer frente a las solicitudes relacionadas con las TIC;
> La adopción de mecanismos nacionales de carácter voluntario para clasificar los incidentes relacionados con las TIC en función de la escala y de la gravedad de esos hechos, a fin de fomentar el intercambio de información sobre ellos.[120]

La Teoría de la Globalización y la Teoría de Complejos de Seguridad Regional, permiten explicar las premisas anteriores debido a que considera el establecimiento de canales de comunicaciones regionales, subregionales y bilaterales para hacer frente a los incidentes informáticos por el uso indebido de las TIC. En ese tenor, se infiere la importancia de la cooperación y el trabajo en conjunto para fortalecer los mecanismos de seguridad y, en este sentido, está el caso de la ciberseguridad. En lo que respecta a México, las condiciones geográficas y políticas, permiten establecer diálogo con la región de América del Norte, de modo que, se pueden lograr grandes avances en materia de intercambio de experiencias, información y desarrollo de capacidades en dicho tema.

En lo que respecta al bienio 2016-2017, se creó un nuevo Grupo de Expertos Gubernamentales para dar seguimiento a los resultados del informe 2014-2015; sin embargo, no se han presentado nuevos estudios. De acuerdo al sitio web de la UNODA, su

[119] "Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, Naciones Unidas. Asamblea General,* A/70/174*,* acceso el 18 de septiembre de 2018 en: http://bit.ly/2lHrVcK
[120] Ibíd.

primera reunión se llevó a cabo en Nueva York en el año 2016, siendo ésta la última información disponible sobre los avances del GEG.

Es oportuno enfatizar que los trabajos de la ONU, en especial de la UNODA, han fortalecido la discusión de la ciberseguridad, al abordar el tema de los sistemas de información en el plano cibernético, toda vez que la base de sus estudios es el mantenimiento de la paz y seguridad internacionales. Por otra parte, el centro de la discusión se lleva a cabo en el seno de la Asamblea General de las Naciones Unidas, por lo que el tema sigue en constante actualización.

Es notable la preocupación de la ONU en el tema de la ciberseguridad, pues los informes que ha realizado el GEG, demuestran que las amenazas y riesgos en el ciberespacio pueden perjudicar la seguridad nacional de los Estados, así como la estabilidad del sistema internacional, especialmente, si se consideran los avances tecnológicos-digitales a nivel planetario.

2.2 La Unión Internacional de Telecomunicaciones

Un organismo especializado de las Naciones Unidas encargado de innovar y mejorar las TIC, es la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés). Está conformada por miembros del sector público (193 Estados de la ONU) y privado (aproximadamente 700 compañías tecnológicas).[121]

Las actividades de la ITU tienen como objetivo reunir a los sectores antes mencionados, con el fin de generar un espacio en el que puedan entablar diálogo, y con ello, establecer acuerdos de cooperación. De tal manera que, se desarrollan conferencias y reuniones para presentar informes, estudios y avances sobre innovación en el ámbito de las TIC.

Para llevar a cabo dichas actividades, la Unión tiene tres agrupaciones que realizan acciones específicas, por lo que se dividen en comisiones de estudio, grupos temáticos y un punto de reunión global.

Las comisiones están conformadas por expertos y especialistas en un tema determinado, por lo que desarrollan estudios y análisis en materia de las TIC. Los resultados de sus

[121] "Visión General", *Unión Internacional de Telecomunicaciones*, acceso el 18 de septiembre de 2018 en: http://bit.ly/2kaJbqd

informes, se convierten en directrices y normas técnicas que son recomendaciones a seguir para el sector público y privado. Por otra parte, la función de los grupos temáticos consiste en realizar reuniones a través de foros, conferencias y mesas de análisis, que tienen como propósito dar a conocer a los miembros de la ITU, los principales avances en el ámbito de las TIC. Por último, el punto de reunión global tiene como objetivo, congregar a los sectores públicos y privados más influyentes para intercambiar conocimientos e información.[122]

Además, la Unión es impulsora de iniciativas que buscan reducir la brecha digital entre los países, para que las personas tengan acceso a tecnologías como el *Internet*. Con base en ello, también realiza estadísticas que miden el nivel de los Estados para determinar el grado de desarrollo de las Tecnologías de la Información y la Comunicación.

Uno de estos mecanismos de medición, es el Índice Mundial de Ciberseguridad (IMC),[123] el cual, es publicado de manera anual, y detalla los principales problemas y vulnerabilidades que tienen las Naciones en materia de seguridad cibernética.

Por lo tanto, se establece que el objetivo central del IMC, consiste en ayudar a los países a identificar áreas de mejora en el campo de la seguridad cibernética para que puedan implementar medidas que fortalezcan sus niveles de ciberseguridad, y con ello, mejoren su posición en la clasificación del índice.[124]

En ese orden de ideas, se desprenden cuatro objetivos principales para la medición del IMC, siendo los siguientes:

- El nivel y evolución que han tenido los países en su compromiso de desarrollar mejores mecanismos de ciberseguridad, en relación con otros;
- el avance de la ciberseguridad de todos los Estados, tomando como referencia una perspectiva global;
- el progreso de la ciberseguridad desde una perspectiva regional;

[122] "¿Qué hace la UIT?", *Unión Internacional de Telecomunicaciones*, s.f., acceso el 18 de septiembre de 2018 en: http://bit.ly/2mbXqfd

[123] El Índice Mundial de Ciberseguridad de 2017 tiene cinco pilares de investigación: aspectos legales, técnicos, organizacionales, cooperación internacional y capacidad de construir cultura de ciberseguridad. En "Índice Global de Ciberseguridad 2017", *Foro Jurídico*, 5 de julio de 2018, acceso el día 18 de septiembre de 2018 en: http://bit.ly/2kFW8Zh

[124] "Global Cybersecurity Index 2017", *International Telecommunication Union*, 2017, p. 4, http://bit.ly/2kD8GRj

- el compromiso de las Naciones en seguridad cibernética en términos de participación e iniciativas sobre el desarrollo de ciberseguridad.[125]

Al fijar parámetros para medir la ciberseguridad, los Estados pueden identificar cuáles han sido sus avances y rezagos en la formulación de iniciativas, estrategias y mecanismos que sirvan de herramientas para enfrentar los problemas que se encuentran en el ciberespacio. Por lo tanto, el aspecto comparativo puede ser visto desde una perspectiva global, regional e incluso bilateral, para atender sus deficiencias o fortalecer sus capacidades, de acuerdo a los cinco pilares de investigación del IMC.

Los tres sectores que la ITU desarrolla son: radiocomunicaciones, normalización y desarrollo. En lo que refiere al primero, se encarga de coordinar y gestionar el espectro de frecuencias eléctricas y las orbitas de los satélites; el segundo, elabora normas que sirven de recomendaciones para los Estados y sector privado en el ámbito de las TIC,[126] y finalmente, el tercero, impulsa iniciativas para que tales tecnologías estén al alcance de la mayoría de las personas, de tal manera que tengan acceso a medios digitales.[127]

Otra contribución que hizo la Unión, fue precisar una definición sobre lo que es la ciberseguridad a través de la Resolución 181, derivado de las decisiones tomadas en la conferencia llevada a cabo en Guadalajara en el año 2010. Además, en la Resolución 130 de ese mismo año, se especifican los asuntos sobre la jurisdicción nacional, determinando que la ITU sólo puede cooperar con los Estados en temas técnicos. De modo que, se establece un marco de referencia en el que la Unión Internacional de Telecomunicaciones, no puede inmiscuirse en asuntos de seguridad y defensa nacional.[128]

Es importante analizar las actividades de la ITU porque desde sus atribuciones, aborda el tema de la ciberseguridad mediante una visión técnica, que tiene como propósito hacer que las TIC funcionen adecuadamente, y estén al alcance de la mayoría de la población mundial. Además, brinda soporte técnico a los Estados que lo soliciten, ya sea en la capacitación de personal, o en la elaboración de recomendaciones. Por otra parte, cabe destacar que reúne a los sectores públicos y privados más influyentes, lo que permite la interacción con otros

[125] Ibíd., p. 3.
[126] Cada año, la UIT elabora y revisa aproximadamente 150 normas que tengan que ver con las TIC.
[127] "¿Qué hace la UIT?...".
[128] "Actualidades de la UIT", *Unión Internacional de Telecomunicaciones*, 2010, p. 21, http://bit.ly/2m8ukgB

actores que requieran desarrollar sus niveles de ciberseguridad, de tal manera que pueden crear vías de comunicación, que den como resultado, un mecanismo de cooperación bilateral o regional con un Estado o empresa.

2.3 La Unión Europea

La Unión Europea (UE), es una asociación económica y política que está compuesta por 28 Estados miembros. A través de la integración, fomentan la competitividad en diversos sectores para fortalecer sus economías, la seguridad y la cooperación, en aras de crear áreas de oportunidad y atenuar problemas comunes.[129]

Promueve el libre flujo de personas, bienes y servicios para dinamizar el intercambio de recursos. El objetivo es elevar los niveles de vida de las personas mediante un incremento en la innovación tecnológica para que ésta contribuya a mejorar la economía, no obstante, dichos avances también generan progreso en materia de seguridad.

La dimensión de los Estados que la integran requiere del trabajo de muchos mecanismos e instituciones para hacer frente a potenciales riesgos que se pueden originar por la magnitud que representa el intercambio de servicios y el flujo de información, que se desarrolla a través de los sistemas informáticos de personas, empresas e instituciones gubernamentales.

En el año 2003, el Consejo Europeo aprobó la Estrategia Europea de Seguridad (EES), que tenía como referente el marco de la Política Común de Seguridad y Defensa del año 1999. Dicha base, enmarca las principales amenazas que la UE podría afrontar; siendo el terrorismo, la proliferación de armas de destrucción masiva, los conflictos regionales, la delincuencia organizada y los Estados Nación, los riesgos más importantes. No obstante, no se mencionaba nada en lo referente al ciberespacio.[130]

Para el año 2004, se crea la Agencia de Seguridad de las Redes y la Información (ENISA, por sus siglas en inglés), para brindar soporte especializado en materia de ciberseguridad, con el fin de prevenir y detectar incidentes informáticos. Las funciones de la agencia, son:

[129] Se enlistan los 28 Estados por año de entrada: Alemania, Bélgica, Francia, Italia, Luxemburgo, Países Bajos (1958); Dinamarca, Irlanda y Reino Unido (1973); Grecia (1981); España y Portugal (1986); Austria, Finlandia y Suecia (1995); Chequia, Chipre, Eslovaquia, Eslovenia, Estonia, Hungría, Letonia, Malta, Lituania y Polonia (2004); Bulgaria y Rumanía (2007) y Croacia en 2013. En "Países", *Unión Europea*, s.f., acceso el 20 de septiembre de 2018 en: http://bit.ly/2lJ2Iys

[130] Nieva Machín y Manuel Gazapo, "La ciberseguridad como factor crítico en la seguridad de la Unión Europea", *Revista UNISCI*, n.°42, 2016, p. 59, http://bit.ly/2kfTN7q

- Gestionar crisis cibernéticas en la Unión Europea, a través de la organización de ejercicios;
- aportar, desde sus atribuciones, al desarrollo de estrategias nacionales de seguridad cibernética, y;
- promover la cooperación entre los equipos de respuesta a incidentes informáticos, así como crear capacidades para atenuar riesgos.[131]

ENISA ayuda a crear mecanismos que estudien y analicen oportunidades de desarrollo en el ámbito de las TIC, con el fin de elaborar estrategias nacionales de ciberseguridad. En ese tenor, países como España, Alemania, Francia, Estonia, entre otros, han instrumentado dichas estrategias en sus agendas de desarrollo. El progreso tecnológico y la incursión digital, han acelerado el establecimiento de normas más estrictas en materia de seguridad cibernética, pues gran parte de sus actividades se llevan a cabo en sistemas informáticos.

Esta agencia rectora en la protección de las redes y la información, proporcionó a la Unión Europea y a los Estados miembros, una perspectiva a mediano y largo plazo sobre los posibles riesgos que podrían materializarse en el ciberespacio. Al entender la importancia vital de los sistemas informáticos, ENISA impulsó la creación del Programa Europeo para la Protección de las Infraestructuras Críticas en el año 2007.[132]

El rol de las infraestructuras críticas para la UE es fundamental, puesto que permiten la correcta operatividad de la mayor parte de los servicios que ofrecen empresas e instituciones gubernamentales en el ámbito de la salud, energías, control de aguas, entre otros. Derivado de esto, el enfoque que destaca sobre la ciberseguridad de la Unión, es el económico, debido a que ha implementado las TIC con el objetivo de dinamizar la productividad de la industria y la sociedad.

En el año 2010, se creó la Agenda Digital[133] para Europa, teniendo como hoja de ruta el crecimiento económico con la aplicación e implementación de una economía interconectada

[131] "Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA)", *Unión Europea*, s.f., acceso el 20 de septiembre de 2018 en: http://bit.ly/2IH9cht

[132] Machín y Gazapo, "La ciberseguridad como factor…", p. 59.

[133] La Agenda Digital para Europa se basa en siete campos de acción: 1) el mercado digital en todos sus espectros; 2) la interoperabilidad y los estándares que dan pie a una democracia digital; 3) la seguridad en el ciberespacio; 4) la velocidad de los accesos a internet; 5) la investigación y la innovación en la TIC; 6) el acceso e inclusión para toda la población y 7) lo digital como beneficio social. Ibíd., p. 60.

digitalmente, pues se considera la conectividad como un punto de enlace que armoniza las transacciones financieras, logísticas e industriales con el uso del *Internet*, la banda ancha y otros elementos que incrementen la productividad.[134] En ese mismo año, se aprobó la Estrategia de Seguridad Interior de la Unión Europea, la cual busca hacer frente a la ciberdelincuencia, porque se considera una amenaza grave para los ciudadanos y la economía digital.[135]

La apuesta de la UE consiste en armonizar lo digital con lo económico, para enfatizar esto, cabe destacar la creación del Mercado Único Digital (MUD), como elemento integrador a la economía digital. El objetivo es llevar a cabo la transición digital en la industria y la sociedad. Con base en lo anterior, los objetivos del MUD referentes a la ciberseguridad, son:

- Actualizar las normas sobre derechos de autor para que se adapten a la era digital;
- fortalecer ENISA para mejorar la respuesta de la Unión Europea ante ciberataques, así como generar una respuesta eficiente en la utilización del derecho penal contra la ciberdelincuencia para proteger a los ciudadanos, empresas e instituciones públicas;
- garantizar una mejor conexión a Internet para que la sociedad pueda participar de manera plena en la economía digital;
- adaptar las reglas sobre *ePrivacy* al nuevo entorno digital;
- auxiliar a las grandes y pequeñas empresas, investigadores, ciudadanos y autoridades públicas a que aprovechen el potencial de las nuevas tecnologías, pero garantizando la enseñanza de una cultura cibernética para que tengan las habilidades necesarias del entorno digital.[136]

Por otra parte, en el año 2013 se creó la Estrategia de Ciberseguridad de la Unión Europea denominada «Un ciberespacio abierto, protegido y seguro», que busca reducir la ciberdelincuencia en la red. La estrategia tiene cinco prioridades, las cuales son:

- La ciberresiliencia;
- reducir la delincuencia en la red;

[134] Comisión Europea, "Agenda Digital para Europa", *Unión Europea*, 2014, p. 3, http://bit.ly/2mbboOo
[135] Luis Feliu, "La ciberseguridad y defensa", en *Monografías del CESEDEN 126*, 2012, p. 64, http://bit.ly/2m3RGUz
[136] "Digital Single Market", *European Commission*, s.f., acceso el 20 de septiembre de 2018 en: http://bit.ly/2kaebXl

- desarrollar una política de ciberdefensa de acuerdo a las capacidades en el rubro de la Política Común de Seguridad y Defensa (PCSD);
- desarrollar recursos tecnológicos e industriales para fortalecer la ciberseguridad;
- establecer una política internacional sobre el ciberespacio en la Unión Europea, la cual promueva los valores europeos esenciales.[137]

Dichos puntos, representan los valores de la Unión Europea para afrontar los riesgos de la ciberdelincuencia, debido a que toma como referencia a la democracia, la libertad y la economía, de ahí que introduzca el concepto de ciberresilencia. También fomenta la necesidad de crear capacidades para desarrollar estrategias y políticas que hagan posible atenuar riesgos. Con base en ello, es preciso destacar la creación de la Directiva sobre Seguridad de las Redes y la Información (NIS, por sus siglas en inglés), como complemento a lo anteriormente establecido en materia de ciberseguridad, pues su aplicación es obligatoria para todos los Estados miembros.

La Directiva NIS, es una normativa de la Unión Europea que pretende mejorar la seguridad de las redes y los sistemas de información en cada uno de los Estados, por lo que resulta imprescindible su implementación en los ordenamientos jurídicos nacionales de los miembros que la conforman.[138]

Las medidas que se deben ejecutar, son las siguientes:

- Establecer obligaciones para todos los Estados miembros en busca de adoptar una estrategia nacional sobre la seguridad de redes y sistemas de información.
- Crear un grupo de cooperación estratégica e intercambio de información entre los Estados miembros.
- Crear una red de Equipos de Respuesta a Incidentes de Seguridad Informática (red CSIRT, por sus siglas en inglés), para mejorar la rapidez y eficacia de la cooperación operativa.

[137] "Plan de ciberseguridad de la UE para proteger una red abierta plena de libertad y de oportunidades en línea", *Comisión Europea*, 07 de febrero de 2013, acceso el 20 de septiembre de 2018 en: http://bit.ly/2lPGf2D

[138] Lucía Gastón, "Qué es la Directiva NIS", *BBVA*, 26 de marzo de 2018, acceso el 20 de septiembre de 2018 en: https://bbva.info/2m3RKnh

- Establecer y notificar los requisitos de seguridad para operadores de servicios esenciales (como el energético, financiero, salud, etc.) y proveedores de servicios digitales (como motores de búsqueda, comercio electrónico o cómputo en la nube).
- Determinar obligaciones para las autoridades nacionales competentes de cada Estado miembro, de los puntos de contacto únicos y los CSIRT, en las tareas relacionadas con la seguridad de redes y sistemas de información.[139]

El propósito de la Directiva NIS es brindar estabilidad al mercado interno, pues lo que se pretende es dar certidumbre a la transición que presenta el Mercado Único Digital. En tal sentido, la UE planea seguir desarrollando estrategias que fortalezcan todo lo que se ha implementado para el buen funcionamiento del sistema económico, particularmente lo que concierne a las actividades digitales.

Aunado a las medidas implementadas para fortalecer la ciberseguridad, la UE considera como propuesta ampliar el alcance y competencia de la ENISA para extender sus funciones, con el objetivo de que analice la certificación de productos en el ámbito de las TIC. Por lo anterior, la nueva denominación de ENISA sería Agencia Europea de Ciberseguridad.[140]

Cabe destacar que la ciberseguridad en la UE se basa en la integración y prosperidad económica, por lo que su enfoque se centra en la transición de la industria y servicios hacia el ámbito digital, tal y como lo demuestra la aplicación de la Agenda Digital y el Mercado Único Digital. En ese sentido, desde la conformación de ENISA en el año 2004 hasta su posible reforma, se muestra el compromiso y los avances de la UE en dicha materia.

2.4 La Organización del Tratado del Atlántico Norte

La Organización del Tratado del Atlántico Norte (OTAN) es una alianza político-militar, que se constituyó a raíz de la firma del tratado de Washington, en el año de 1949. El inicio de la Guerra Fría y la defensa colectiva, forjaron los fundamentos de la organización para responder ante una posible agresión armada. Sin embargo, los cambios en el sistema internacional provocados por el fin de la confrontación político-militar, aunado al desarrollo

[139] Miguel Mendoza, "NIS: ¿qué es y qué implica esta nueva legislación en seguridad?", *Welivesecurity by eset*, 22 de julio de 2016, acceso el 20 de septiembre de 2018 en: http://bit.ly/2ktzrrs

[140] "Nuevas Medidas para reforzar la ciberseguridad en Europa", *Centro Criptológico Nacional*, 21 de septiembre de 2017, acceso el 20 de septiembre de 2018 en: http://bit.ly/2lH9mW7

de nuevas tecnologías y planes estratégicos, han obligado a que la alianza se adapte a la coyuntura del siglo XXI.[141]

El organismo regional está conformado por 29 Estados miembros[142] y enlazan a Europa y América del Norte (Estados Unidos y Canadá), por lo que sus integrantes expanden su zona de operatividad e influyen en los asuntos de seguridad y defensa, de acuerdo a los intereses que tengan en común.

La importancia estratégica de la OTAN, reside en los artículos 5 y 6 del tratado fundacional, que a la letra dicen:

> Artículo 5. Las partes convienen en que un ataque armado contra una o contra varias de ellas, acaecido en Europa o en América del Norte, se considerará como un ataque dirigido contra todas ellas y, en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva, reconocido por el artículo 51 de la Carta de las Naciones Unidas, asistirá a la Parte o Partes así atacadas, adoptando seguidamente, individualmente y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer y mantener la seguridad en la región del Atlántico Norte.
>
> Todo ataque armado de esta naturaleza y toda medida adoptada en consecuencia se pondrán, inmediatamente, en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las medidas necesarias para restablecer y mantener la paz y la seguridad internacionales.
>
> Artículo 6. A efectos del artículo 5 se considera ataque armado contra una o varias de las Partes:
>
> a) Contra el territorio de cualquiera de las partes en Europa o en América del Norte…, contra el territorio de Turquía o contra las islas bajo jurisdicción de cualquiera de las partes en la región del Atlántico Norte al norte del Trópico de Cáncer; b) Contra las fuerzas, buques o aeronaves de cualquiera de las partes que están en dichos territorios o sobre ellos, o en cualquiera otra región de Europa en la que estuviesen estacionadas fuerzas de ocupación de cualquiera de las partes en la fecha en que el Tratado entró en vigor, o en el mar Mediterráneo, o en la región del Atlántico Norte, al norte del Trópico de Cáncer.[143]

---

[141] Gobierno de España, "¿Qué es la Alianza Atlántica, qué es la OTAN?", *Ministerio de Asuntos Exteriores y de Cooperación*, 20 de abril de 2015, acceso el 20 de septiembre de 2018 en: http://bit.ly/2mbbIN6

[142] Se enlistan los 29 Estados por año de entrada: Bélgica, Canadá, Dinamarca, Francia, Islandia, Italia, Luxemburgo, Países Bajos, Noruega, Portugal, Reino Unido y Estados Unidos (1949); Grecia y Turquía (1952); Alemania (1955); España (1982); República Checa, Hungría y Polonia (1999); Bulgaria, Estonia, Letonia, Lituania, Rumanía, Eslovaquia, Eslovenia (2004); Albania y Croacia (2009), y Montenegro en 2017. En "Estados Miembros", *NATO/OTAN*, s.f., acceso el 20 de septiembre de 2018 en: http://bit.ly/2kFCTz3

[143] "Seguridad colectiva", *Ministerio de Asuntos Exteriores y Cooperación*, 20 de abril de 2015, acceso el 20 de septiembre de 2018 en: http://bit.ly/2ke7aoD

Dichos artículos son pieza clave para comprender la alianza de los Estados integrantes, y con ello, entender las redefiniciones de conceptos y políticas, que deriven en la aplicación de nuevos marcos de acción en la defensa colectiva. El aspecto conceptual adquiere gran relevancia en el ámbito del ciberespacio, pues a partir de ello se establecerán las líneas de acción que den sustento a la seguridad y defensa de la organización.

La OTAN, a comparación del pasado siglo, ha incrementado su gasto militar gradualmente, y con base en ello, ha creado agencias y centros especializados que tienen como objetivo, innovar tecnológicamente la seguridad y la defensa de la organización, así como la de los Estados miembros. De acuerdo al sitio web de la OTAN, las agencias que tratan el tema de la ciberseguridad y ciberdefensa son: el Comité Asesor de Guerra Electrónica (NATO Electronic Warfare Advisory Comitte, NEWAC), el cual atiende los asuntos de guerra electrónica; por otra parte, también cuenta con la Escuela de Sistemas de Información y Comunicaciones (NATO Communications and Information Systems School), que se encarga de educar y entrenar a personal en ese rubro. Por último, está el Centro de Excelencia de Defensa Cibernética Cooperativa (CCDCOE, por sus siglas en inglés), que tiene como función generar estudios en la materia, así como brindar soporte a los Estados que lo soliciten.[144]

Cuando Estonia se unió en el año 2004, propuso a la OTAN crear un Centro de Defensa Cibernético para desarrollar estrategias en el ciberespacio. Sin embargo, trascurrieron cuatro años para que el Consejo del Atlántico Norte aprobará la acreditación[145] del CCDCOE.[146]

En el año 2008 se establecieron dos mecanismos para abordar los riesgos en el ciberespacio;[147] el primero, fue la acreditación del CCDCOE, y el segundo fue la firma de la

[144] "NATO Organization", *North Atlantic Treaty Organization NATO/OTAN*, s.f., acceso el 20 de septiembre de 2018 en: http://bit.ly/2mbYOyx

[145] El Centro fue creado por siete naciones (Estonia, Alemania, Italia, Lituania, Letonia, República Eslovaca y España) mediante la celebración de un Memorando de Entendimiento; sin embargo, el Consejo del Atlántico Norte otorgó el estatus de Organización Militar Internacional, reafirmando su acreditación ante la OTAN. En "Centre is the first International Military Organization hosted by Estonia", *NATO Cooperative Cyber Defence Centre of Excellence*, s.f., acceso el 20 de septiembre de 2018 en: http://bit.ly/2ktA1Wa

[146] "History", *NATO Cooperative Cyber Defence Centre of Excellence*, s.f., acceso el 20 de septiembre de 2018 en: http://bit.ly/2lJXxye

[147] La OTAN no supo cómo responder ante los ciberataques que recibió Estonia en el año 2007, debido a que no se tenía un plan de acción para hacer frente a incidentes cibernéticos. En Néstor Ganuza, "La situación de la ciberseguridad en el ámbito internacional y en la OTAN", en *Cuadernos de Estrategia 149*, 2010, p. 204, http://bit.ly/2mb0x77

Política de Ciberdefensa, esto con el propósito de fortalecer y mejorar la capacidad para proteger los sistemas de información y comunicaciones que tuvieran una importancia vital para la OTAN contra ciberataques.[148]

Además, en ese mismo año, se llevó a cabo la Cumbre de Bucarest, donde se especificó la necesidad de contar con una política para la defensa del ciberespacio, declarando, en la sección 47, lo siguiente:

> La OTAN se mantiene comprometida con el fortalecimiento de los sistemas de información crítica de la Alianza contra ciberataques. Hemos adoptados recientemente la Política de Ciberdefensa, y estamos desarrollando las estructuras y autoridades para llevarla a cabo. Nuestra política en materia de Ciberdefensa subraya la necesidad de la OTAN y de las naciones miembros de proteger los sistemas de información crítica conforme con sus respectivas responsabilidades; compartir las mejores prácticas y establecer una capacidad de apoyo a las naciones, bajo petición, para contrarrestar un ciberataque. Continuamos con el desarrollo de las capacidades de ciberdefensa de la OTAN y con el fortalecimiento de los vínculos entre la OTAN y las autoridades nacionales.[149]

Los anteriores sucesos marcaron un hito en la definición de la política de ciberdefensa, que en relación con el trabajo del CCDCOE, forman las bases para tratar el tema en la Cumbre de Lisboa del año 2010. En dicha cumbre, adoptan el Nuevo Concepto Estratégico (NCE), en donde definen los nuevos retos globales que la OTAN tendrá que afrontar, siendo uno de éstos, los ciberataques.

El NCE considera que los ciberataques cada vez adquieren mayor dinamismo, al ser más frecuentes, representan un riesgo para los Estados y la Organización, pues consideran que pueden causar inestabilidad en los Estados miembros. Los impactos negativos podrían tener efecto en los individuos y también en las infraestructuras críticas, por lo que la seguridad y prosperidad de la OTAN se verían afectadas.[150]

Sumado a lo anterior, en el año 2011 se aprobó la instrumentación de una Nueva Política de Ciberdefensa, en la que se estipula que la infraestructura y redes de la OTAN, adquieren un grado crítico. En ese tenor, se vuelve necesario dotarles de protección cibernética para poder

[148] Ibíd.
[149] Ibíd., p. 203.
[150] "Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization", *NATO,* Summit in Lisbon, 2010, p. 11, http://bit.ly/2kafjKz

realizar las actividades diarias, en especial las que tienen como misión la defensa colectiva y la gestión de crisis.[151]

La Cumbre de Lisboa y la Nueva Política de Ciberdefensa, le confieren el poder al Consejo del Atlántico Norte para deliberar en qué momento se puede declarar un asunto como defensa colectiva, y con ello, activar el artículo 5 de la OTAN. De esta manera, ante un ataque cibernético, se puede decretar la defensa colectiva, siempre y cuando, el Consejo lo apruebe.[152]

En la Cumbre de Varsovia del año 2016, la OTAN incluyó al ciberespacio como un nuevo dominio de operaciones, al igual que la tierra, el mar y el aire. Además, declaró que se mejorarían las políticas y capacidades nacionales de los Estados miembros para cumplir con el Compromiso en Cibedefensa[153] (Ciber Defence Pledge), con el propósito de que sus estrategias estén a la vanguardia en contra de las amenazas cibernéticas, pues como es sabido, las acciones ofensivas en forma de códigos maliciosos están en constante actualización, por lo que la defensa también debe estarlo, especialmente, la colectiva.

El avance significativo de la ciberseguridad desde una arista político-militar, se puede explicar mediante la Teoría de Complejos de Seguridad Regional, al contemplar los asuntos regionales y globales. Además, el objeto referente de la securitización, pone en evidencia que la ciberdefensa se vuelve una nueva dimensión de operaciones. En ese sentido, se infiere que el agente securitizador es la OTAN, pues las cumbres, los anuncios de las políticas y lo acontecido en Estonia, son las bases que dan sustento para categorizar al ciberespacio como un factor de riesgo que puede tener impactos negativos en la prosperidad, estabilidad y seguridad de la organización.

Desde la Cumbre de Bucarest hasta la de Varsovia, y la definición del NCE, se clasifican la ciberseguridad y la ciberdefensa como asuntos críticos que deben ser desarrollados para proteger los intereses de la organización. Por lo tanto, se cumple con el proceso de securitización en la OTAN, tal y como lo establecen los Complejos de Seguridad Regional.

---

[151] Carlos Enríquez, "Estrategias internacionales para el ciberespacio", en *Monografías del CESEDEN 126*, 2012, p. 102, http://bit.ly/2m3RGUz

[152] Ibíd.

[153] Juan Moliner, "La Cumbre de la OTAN en Varsovia", *Instituto Español de Estudios Estratégicos*, opinión 79bis/2016, 2016, pp. 8-9, http://bit.ly/2kD9WE1

2.5 La Organización de los Estados Americanos

La Organización de los Estados Americanos (OEA), se creó en el año de 1948 mediante la suscripción de la Carta de la OEA; sin embargo, entró en vigor hasta 1951. Cabe destacar que la Carta original ha sido enmendada en cuatro ocasiones por los protocolos de Buenos Aires (1970), Cartagena de Indias (1988), Managua (1996) y el de Washington (1997).[154] Los pilares que dan sustento a la OEA son la democracia, los derechos humanos, la seguridad y el desarrollo; por lo que, sus estudios, políticas y resoluciones, tienen como base central dichos temas. Por otra parte, son 35 Estados miembros los que conforman la organización.[155]

En lo que respecta a los asuntos de seguridad, el propósito esencial es lograr la paz y la seguridad del continente, así como prevenir las causas que susciten conflictos entre los Estados miembros, procurando siempre la solución pacífica de las controversias. Además, promueve, mediante la cooperación, el desarrollo económico, social y cultural.[156]

La OEA procura mantener el bienestar y la estabilidad de los Estados miembros para que exista, a nivel continental, un entorno de paz y seguridad. En este sentido, el asunto de la ciberseguridad es atendido y desarrollado por la Secretaría de Seguridad Multidimensional (SSM), debido al enfoque múltiple que tiene sobre los riesgos y las amenazas.

La SSM tiene como eje de acción la Declaración sobre Seguridad de las Américas, celebreda en el año 2003, en la que dimensionan, desde un criterio amplio, las amenazas tradicionales, así como el surgimiento de nuevas que puedan afectar el orden público de los Estados. Por lo tanto, la declaración establece como desafíos de naturaleza diversa, los siguientes:

- El terrorismo, la delincuencia organizada transnacional, la problemática de las drogas, la corrupción, el lavado de activos y el tráfico ilícito de armas;

[154] "Quiénes somos", *Organización de los Estados Americanos*, s.f., acceso el 23 de septiembre de 2018 en: http://bit.ly/2lNEdA4

[155] Se enlistan los Estados por año de entrada: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba (la Resolución AG/RES.2438 (XXXIX-O/09) resuelve que Cuba no puede ser participe en el sistema interamericano), Ecuador, El Salvador, Estados Unidos de América, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay (1948); Barbados, Trinidad y Tobago (1967); Jamaica (1969); Grenada (1975); Suriname (1977); Dominica, Santa Lucía (1979); Antigua y Barbuda, San Vicente y las Granadinas (1981); Bahamas (1982); St. Kitts y Nevis (1984); Canadá (1990); Belize y Guyana (1991). En "Estados Miembros", *Organización de los Estados Americanos*, s.f., acceso el 23 de septiembre de 2018 en: http://bit.ly/2k6qALU

[156] "Nuestro Propósito", *Organización de los Estados Americanos*, s.f., acceso el 23 de septiembre de 2018 en: http://bit.ly/2ke7CmP

- la pobreza extrema y la exclusión social de amplios sectores de la población pueden erosionar y vulnerar la seguridad de los Estados conforme aumenta;
- el deterioro del medio ambiente, que puede inferir en los desastres naturales. Por otra parte, las enfermedades como el VIH/SIDA, también pueden repercutir en la seguridad;
- la trata de personas;
- los ataques a la seguridad cibernética;
- el riesgo posible de que un accidente en el transporte marítimo de materiales potencialmente peligrosos (como materiales radioactivos y desechos tóxicos), que pueden ocasionar una crisis ambiental;
- la posesión de armas de destrucción masiva y su posible uso por parte de Estados u organizaciones terroristas.[157]

En ese orden de ideas, la Declaración hace mención de que la cooperación es un instrumento necesario para que los Estados puedan afrontar los desafíos de naturaleza diversa. Con ello, destaca el criterio de integración regional y subregional en el ámbito de la seguridad y defensa como una estrategia para fortalecer la seguridad en el hemisferio.[158]

La SSM está compuesta por cuatro dependencias que tratan de manera especializada diversos temas y que tienen como eje rector la Declaración antes mencionada. La primera es la Secretaría Ejecutiva de la Comisión Interamericana para el Control del Abuso de Drogas; la segunda es la Secretaría del Comité Interamericano Contra el Terrorismo; la tercera es el Departamento de Seguridad Púbica; y la cuarta es el Departamento contra la Delincuencia Organizada Transnacional.

El aspecto de la seguridad cibernética y la protección de infraestructura crítica le competen a la Secretaría del Comité Interamericano Contra el Terrorismo (CICTE), por lo que sus funciones derivan de apoyar a los Estados miembros con el fortalecimiento de sus capacidades a través de asistencia y soporte técnico, de acuerdo a las necesidades y solicitudes que hagan al Comité.

[157] "Declaración sobre seguridad en las Américas", *Organización de los Estados Americanos*, 2003, p. 4, http://bit.ly/2kfVEZW
[158] Ibíd., p. 5.

CUADRO 5. ORGANIGRAMA DE LA SECRETARÍA DE SEGURIDAD MULTIDIMENSIONAL.[159]

La seguridad cibernética ha sido abordada por la OEA desde el año 2003, cuando se aprobó la resolución AG/RES.1939 (XXXIII-O/03), en la que se encomendó desarrollar un proyecto que estudiara la ciberseguridad desde un enfoque multidimensional y multidisciplinario.[160] En el año 2004 se aprobó la resolución AG/RES. 2004 (XXXIV-O/04), que lleva por título «Estrategia Interamericana Integral para combatir las Amenazas a la Seguridad Cibernética», y confiere al CICTE, las competencias para que integre la seguridad cibernética a sus funciones.[161]

Los objetivos de la SSM en el ámbito cibernético son:

- Establecer grupos nacionales de alerta, vigilancia y prevención, denominados Equipos de Respuesta a Incidentes (CSIRT, por sus siglas en inglés);
- crear una red de alerta Hemisférica que proporcione formación técnica a personal que trabaje en la seguridad cibernética de los gobiernos;

[159] "Secretaría de Seguridad Multidimensional", Organización de Estados Americanos, s.f., acceso el 23 de septiembre de 2018 en: http://bit.ly/2ktAyHE
[160] "Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética", *Organización de los Estados Americanos*, 10 de junio de 2003, acceso el 23 de septiembre de 2018 en: http://bit.ly/2lOVR6t
[161] "Seguridad Cibernética", *Organización de los Estados Americanos*, s.f., acceso el 23 de septiembre de 2018 en: http://bit.ly/2kDar0R

- fomentar el desarrollo de Estrategias Nacionales sobre seguridad cibernética;
- promover una cultura en seguridad cibernética que permita desarrollar conocimiento.[162]

En esa tesitura, México tiene registrados ante la SSM, cuatro Equipos de Respuesta ante Emergencias Informáticas (CERTS, por sus siglas en inglés), siendo los siguientes:[163]

- Centro Nacional de Respuesta a Incidentes Cibernéticos-Policía Federal de México (CERT-MX);
- equipo de Respuesta a Incidentes de Seguridad Informática de la Universidad Nacional Autónoma de México (UNAM-CERT);
- centro de Respuesta a Incidentes Cibernéticos (MNEMO-CERT), y;
- equipos de Respuesta a Incidentes Cibernéticos (SCITUM-CSIRT).[164]

Para México resulta importante tener registrados CERTS ante la SSM, debido a que puede solicitar la asistencia y soporte técnico que tenga como objetivo fortalecer los mecanismos establecidos en materia de seguridad cibernética, especialmente si se trata de cuestiones técnicas. Además, al hacerlo se estarían cumpliendo dos propósitos; el primero consiste en que México refrenda su compromiso ante la Organización de los Estados Americanos en dicha temática y, por otra parte, incrementa sus capacidades técnicas y operativas en dicha área.

En ese tenor, Alfred Schandlbauer, Secretario Ejecutivo del CICTE, al describir al sitio web *Segurilatam*, explica cómo la OEA brinda soporte en materia de seguridad cibernética, y precisa lo siguiente:

> La OEA apoya a los países en la organización de debates con la participación de interesados claves en seguridad cibernética nacionales, incluyendo representantes gubernamentales, el sector privado, la sociedad civil y la comunidad académica. Facilitadas por nuestros expertos, las sesiones buscan familiarizar a los participantes con el propósito de las estrategias nacionales de ciberseguridad y darles a conocer la función y componentes de una serie de estrategias que están en vigor en todo el mundo.

[162] Ibíd.
[163] Los servicios del CERT-MX y UNAM-CERT tienen circunscripción pública, mientras que MNEMO-CERT y SCITUM-CSIRT pertenecen al sector privado.
[164] "México", *Organización de los Estados Americanos*, s.f., acceso el 23 de septiembre de 2018 en: http://bit.ly/2mb0Ui1

> La OEA organiza la información recopilada y presenta un proyecto de estrategia de los Estados miembros,… y se le presenta a las autoridades competentes para su aprobación.[165]

La explicación de Schandlbauer resulta puntual al esclarecer la manera de trabajo de la OEA. De esta manera, la organización genera debates en la que participan diversos sectores que contribuyen a la formulación de una estrategia nacional de ciberseguridad, en la que se considera el contexto nacional, regional e internacional. Cabe destacar que el documento final es emitido en forma de recomendaciones hacia el gobierno que lo solicitó.

México ya trabajó en conjunto con la OEA para formular una Estrategia Nacional de Ciberseguridad, la cual será analizada en el capítulo 5 de esta investigación. No obstante, es necesario matizar que la organización es una gran impulsora en los asuntos de seguridad multidimensional, particularmente si se menciona el ámbito de la seguridad cibernética.

Los trabajos de la OEA en lo referente a la ciberseguridad resultan esenciales, pues de manera regional, subregional y bilateral, abordan el ámbito de la seguridad cibernética a través de estudios, análisis y resoluciones. En ese sentido, los argumentos de la Teoría de Complejos de Seguridad Regional pueden explicar cómo se ha ido desarrollando el asunto de la ciberseguridad en la organización, y cómo ésta, ha tenido injerencia como agente securitizador en la elaboración de estrategias nacionales de ciberseguridad.

Por otra parte, el aspecto globalizador, en concordancia con la seguridad cibernética, pudo ser abordado a través de las organizaciones internacionales que han desarrollado el tema de acuerdo a sus intereses. En ese tenor, el enfoque particular de cada organización permite explicar de qué manera interpretan las amenazas y riesgos en el ciberespacio, y también cuál es su eje de acción para hacerles frente.

[165] Bernardo Valadés, "Entrevista", *Segurilatam*, 1 de marzo de 2016, acceso el 23 de septiembre de 2018 en: http://bit.ly/2kcM1Lo

CAPÍTULO 3

VULNERABILIDADES A LA CIBERSEGURIDAD

Diversos Estados se encuentran fortaleciendo sus estrategias y políticas de ciberseguridad, algunos apenas las están creando y otros ni siquiera tienen en consideración el tópico en sus agendas de políticas públicas.

Tener una seguridad sólida no significa que se está seguro del todo, porque existe la posibilidad de que se manifieste un ataque, pues siempre hay un punto en el que se puede arremeter contra la integridad de un individuo, empresa, organización o institución gubernamental. La razón es simple, toda defensa tiene un punto ciego, es decir, una vulnerabilidad que el enemigo o delincuente puede aprovechar para llevar a cabo acciones ilícitas.

En tal sentido, la seguridad cibernética también puede llegar a ser debilitada hasta el punto de crear una ruta para acceder a los datos más profundos de un ordenador, sin que el usuario otorgue los permisos necesarios. La razón es simple, en muchas ocasiones los sistemas de un dispositivo electrónico no cuentan con los protocolos de defensa requeridos.

La falta de conocimientos sobre ciberseguridad a nivel general es un factor que perjudica a todos los sectores que componen las actividades productivas y de servicios en un Estado. Las causas más comunes que hacen posible que se reproduzcan efectos negativos, se debe a la inexistencia de legislación, políticas o estrategias que tengan como propósito la defensa de la información y los sistemas informáticos.

Por otra parte, el desarrollo de mecanismos de ciberseguridad para proteger instalaciones estratégicas que tengan componentes que procesen información y códigos, también genera fundamentos para la creación de estrategias ofensivas, pues toda seguridad requiere de procedimientos de respuesta ante una amenaza. En ese sentido, algunos países están desarrollando instrumentos que tienen como propósito fortalecer las capacidades en el ciberespacio desde un enfoque militar, debido a que es considerado como un nuevo espacio para el desarrollo de conflictos bélicos. Diversos expertos y especialistas lo denominan quinto dominio de guerra por la complementariedad que genera a las acciones tradicionales del uso de la fuerza por parte de ejércitos, de modo que permite la aplicación de estrategias combinadas en el ámbito físico y virtual.

3.1 Aproximaciones de la lucha por el quinto dominio

El ciberespacio está siendo considerado como un nuevo entorno que puede servir para atacar a otro enemigo desde lo informático, puesto que los avances tecnológicos conciben nuevos mecanismos más sofisticados que dan impulso a los propósitos de la guerra.

La historia nos permite visualizar cómo los demás dominios fueron agregándose a los objetivos de la lucha armada. El primero, es considerado como la base de todos los demás, debido a que el territorio es donde se encuentran los asentamientos más importantes del Estado, como lo es la población; sin embargo, los otros se crearon como complementos al primero, de modo que el dominio marítimo, aéreo y ultraterrestre se fueron especializando al punto de adquirir un fundamento propio en su desarrollo.

Los promotores de dichos dominios son los Estados, de modo que consideran como punto inicial los fines militares para desarrollar tecnología que les provea de protección y seguridad contra otros sujetos y actores que puedan poner en peligro su integridad territorial.

En este sentido, se crean las condiciones que dan sustento al dilema de la seguridad, de tal manera que otros sujetos también desarrollan capacidades ofensivas y defensivas con el objetivo de equilibrar la balanza de poder para que esto no suponga una amenaza directa a sus intereses e integridad soberana.

A medida que se incrementa el desarrollo de nuevas tecnologías, causa modificaciones en los esquemas tradicionales militares, por lo que se tiende a adaptar las estrategias y doctrinas de acuerdo a la coyuntura nacional, regional e internacional. Aunado a ello, el uso de las TIC facilita el intercambio de información y también impulsa la innovación tecnológica para afrontar nuevos retos en los ámbitos de la seguridad y la defensa. De tal manera que, se ha creado el concepto de Revolución de los Asuntos Militares (RMA, por sus siglas en inglés), que se refiere a la adaptación y evolución de nuevas formas de hacer guerra.[166]

Complementando la idea anterior, Mele manifiesta que desde el año 2007, se fue definiendo en las agendas políticas de los gobiernos, la idea de explotar el ciberespacio para propósitos militares.[167] Esto ha hecho que los ejércitos modernos que emplean un gran número de

[166] Javier Miguel Gil, "La integración del ciberespacio en el ámbito militar", *Universidad de Granada*, 11 de octubre de 2017, acceso el 24 de septiembre de 2018 en: http://bit.ly/2k8PF92

[167] Stefano Mele, "La batalla por el ciberespacio y el ciberarmamento", *Vanguardia Dossier*, n. 54, 2015, p. 29.

soldados, ya no sean suficientes para obtener resultados positivos, porque la revolución tecnológica también afecta al bando más débil, permitiéndoles adquirir la capacidad de infligir daños al adversario más fuerte con un coste menor y sin emplear una milicia con las mismas proporciones.[168] Esto quiere decir que a través del empleo de tecnologías informáticas, tales como el desarrollo de códigos sofisticados, dota, al bando más débil en términos de estructura y recursos militares, el poder de causar un alto daño a las infraestructuras vitales de un Estado.

La realidad es que pequeños grupos pueden causar fuertes daños en comunidades más grandes y preparadas. Basta mencionar como referencia el acaecimiento del 11 de septiembre de 2001 en los Estados Unidos. De modo que el crimen organizado, el terrorismo y otros grupos delictivos pueden tener un potencial alto en la elaboración de estrategias que les permitan utilizar las innovaciones tecnológicas para rivalizar con ejércitos de países más fuertes.

Aunado a lo anterior, Móises Naím específica que:

> En el siglo XXI, el poder ya no es lo que era, pues es más fácil de adquirir, más difícil de utilizar y más fácil de perder. Desde las salas de juntas y las zonas de combate hasta el ciberespacio, las luchas de poder son tan intensas como lo han sido siempre, pero cada vez dan menos resultados.[169]

La fragmentación del poder ha ocasionado que nuevos actores adquieran protagonismo en el escenario internacional. Por tal razón, el ciberespacio es considerado un dominio más en el que todos quieren ejercer control y fuerza. No sólo los Estados y las organizaciones son participes, también delincuentes, terroristas, insurgentes, piratas informáticos, traficantes y ciberdelincuentes encuentran un espacio libre para cometer acciones ilícitas que les permitan adquirir dinero, pero igualmente poder.[170]

Esta lucha se traslada también al ámbito virtual, y en ese tenor, Pérez establece que:

> En esta guerra el gran y único objetivo es el mismo de siempre: el poder. Es una guerra por cambiar el mapa geopolítico mundial, los tradicionales equilibrios de poder establecidos tras la Guerra Fría. Es una guerra que está ganando y ganará el que tenga menos escrúpulos y más concentración de poder.

[168] Móises Naím, *El Fin del Poder*, Debate, México, 2015, p. 23.
[169] Ibíd., p. 18.
[170] Ibíd., p. 32.

> Una guerra que está perdiendo y perderá, por consiguiente, quien subestime esta amenaza.[171]

Tal escenario conlleva a redefinir el esquema de la guerra tradicional. Esto ha hecho posible que los Estados destinen más presupuesto y recursos para el desarrollo del ámbito militar en el ciberespacio, con el fin inmediato de ganar un sitio en relación a los otros actores que también buscan hacerse de un espacio en el mismo. De acuerdo con Mele, Estados como Francia, Alemania, Finlandia y los Países Bajos, ya han anunciado que el ciberespacio es un dominio de guerra. No obstante, Francia y Países Bajos han formalizado, ulteriormente, un pilar estratégico para crear mecanismos de disuasión que les permita prevenir conflictos en el entorno virtual.[172]

En esa tesitura, en el año 2010, el ex subsecretario de Defensa de los Estados Unidos, William J. Lynn, mencionó que el ciberespacio es el quinto dominio de guerra, de modo que «en el siglo XXI, los *bits* y *bytes* pueden ser tan peligrosos como las balas y las bombas».[173] Los datos son un recurso con un gran valor económico, político y militar, pues a partir de ellos, se pueden adquirir enormes ventajas respecto a otros actores.

En el año 2011, la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA, por sus siglas en inglés), se encontraba supervisando el Cibercampo Nacional (NCR, por sus siglas en inglés), en el que se estaba desarrollando un modelo a escala de *Internet* para simular juegos de guerra cibernética, con el fin de prepararse y fortalecer sus defensas en el aspecto informático. En ese mismo año, el Departamento de Defensa de Estados Unidos destinó $500 millones de dólares para el desarrollo de cibertecnologías.[174]

En este sentido, Ventura agrega que:

> La guerra de nuestro tiempo se hace en el mundo virtual. Los ejércitos cibernéticos de Estados Unidos, Rusia y otras potencias como China pugnan, con grandes presupuestos y ejércitos cada vez más numerosos de cibersoldados, por lograr una posición hegemónica de internet… sin embargo, no es un

[171] Jenny Pérez, "Europa y la guerra por el ciberespacio", *Deutsche Welle*, 16 de febrero de 2018, acceso el 24 de septiembre de 2018 en: http://bit.ly/2mad0Ie
[172] Mele, "La batalla por el ciberespacio…", p. 41.
[173] William Márquez, "Ciberespacio: el nuevo ámbito de la guerra para el Pentágono", *BBC Mundo*, 27 de julio de 2011, acceso el 24 de septiembre de 2018 en: https://bbc.in/2lHOM80
[174] "El nuevo campo de entrenamiento para las ciberguerras", *BBC Mundo*, 18 de junio de 2011, acceso el 24 de septiembre de 2018 en: http://bit.ly/2ktD4h6

territorio físico sobre el que poner la bota y clavar la bandera, sino más bien un marco dinámico en el que diariamente surgen fragilidades y desafíos a los que hacer frente.[175]

Hay grandes diferencias entre el arsenal convencional y las armas de destrucción masiva, principalmente, por la cantidad existente y por el daño que puede ocasionar a puntos clave de los componentes de un Estado. En este sentido, es indispensable dimensionar la incorporación del ámbito virtual como una herramienta sofisticada para las acciones bélicas.

CUADRO 6. DIFERENCIAS ENTRE ARMAMENTO NUCLEAR Y CIBERNÉTICO.[176]

Armamento Nuclear	Armamento Cibernético	Categoría
Ya existen trabajos que describen el uso de este armamento	Aún no existe un consenso o definición sobre las armas cibernéticas	Normativa
Se puede tener una estadística de cuántas armas existen	No se puede establecer un registro de la existencia de ciberarmas	Transparencia
El armamento se puede almacenar en un espacio físico y es altamente destructivo	Las ciberarmas se almacenan en un espacio virtual. Sin embargo, importa mucho el factor tiempo, pues pueden perder eficacia	Almacenamiento
Al ser armas físicas, tienen objetivos físicos predeterminados para causar daños potenciales	El aspecto virtual hace posible que los ataques sean instantáneos en un espacio que no tiene fronteras	Geografía
Existen tratados y organizaciones que regulan las armas nucleares	No existen tratados y organismos que regulen la propagación de armas cibernéticas	Acuerdos Internacionales
Tiene repercusiones altas en muchos ámbitos por su alto poder destructivo	Su efecto puede ocasionar repercusiones a gran escala porque tiene un alcance global, sin embargo, no tiene un alto grado de destrucción	Efectos del armamento

Tal y como lo demuestra el cuadro anterior, la creación de armamento cibernético tiene características muy particulares que lo diferencian del arsenal nuclear. Ambos están diseñados para causar destrucción, aunque en distintos niveles. Por otra parte, una

[175] Daniel Ventura, "Ciberguerra: la lucha de las grandes potencias por controlar internet", *Huffpost Español*, 07 de febrero de 2017, acceso el 24 de septiembre de 2018 en: http://bit.ly/2kDaOIN

[176] Elaboración propia con datos obtenidos de Javier Miguel Gil, "La integración del ciberespacio en el ámbito militar", Universidad de Granada, análisis GESI 35/2017, http://bit.ly/2k8PF92

diferencia tajante es que a pesar del tiempo, las armas nucleares siguen siendo peligrosas, mientras que las ciberarmas deben ser actualizadas para que puedan cumplir con su objetivo.

De modo que el desarrollo de capacidades militares en el ciberespacio, requiere de la constante creación y actualización de códigos para promover los intereses bélicos, y con ello, constituir mecanismos de poder cibernético. Es por esto que los Estados y otros actores buscan consolidar un ciberpoder[177] que les permita obtener resultados estratégicos respecto a sus rivales, mediante el desarrollo de armas cibernéticas especializadas con un objetivo determinado. Aunado al ciberpoder, Rosas menciona que «los componentes del poder nacional son dinámicos y cambiantes. En este sentido,… el concepto de ciberpoder… es caracterizado como la capacidad para emplear el ciberespacio a fin de crear ventajas e influir en los acontecimientos en todos los ambientes operativos y en todos los instrumentos del poder».[178]

En forma similar a las armas nucleares y armamento convencional, algunos especialistas y expertos señalan que se debe promover la disuasión en el ciberespacio para evitar que se desarrollen ataques por miedo a las represalias de acuerdo con las capacidades del Estado. Éstas se materializan a través de políticas, estrategias y modelos de seguridad que fortalecen las instituciones encargadas de proveer seguridad y defensa. Además, la coordinación y cooperación con otros Estados y organismos especializados, también complementan la disuasión.

Las características que tiene el ciberespacio posibilitan que el conflicto se extienda, puesto que favorece tanto a los Estados como a los grupos pequeños. De acuerdo con López, las características son:

a) Capilaridad y ubicuidad. Cualquier persona puede tener acceso.
b) Anonimato. Las acciones empleadas son difíciles de rastrear de manera rápida, por lo que la mayor parte de las veces, no se sabe dónde se originó el ataque.

[177] El ciberpoder es definido por Nye como un «conjunto de recursos relacionados con la creación, control y comunicación de información basada en sistemas electrónicos y computacionales… esto incluye no sólo la internet, computadores conectados en red, sino también intranets, tecnología celular y comunicaciones satelitales». En Javier Castrillón-Riascos, "Nada volverá a ser igual: ciberguerra y ciberpoder", *Memorias*, vol. 13, n. 23, 2015, p. 119, http://bit.ly/2mbZrbh

[178] María Cristina Rosas, "Ciberespacio, crimen organizado y seguridad nacional", *América Latina en movimiento*, 08 de mayo de 2011, acceso el 24 de septiembre de 2018 en: http://bit.ly/2lJZ4Eu

c) Eficiencia. Con un costo menor, se puede causar un alto daño.
d) Rendimiento. Al ser llevados a cabo mediante ordenadores y dispositivos, se pueden implementar códigos que hagan tareas múltiples y personalizadas.
e) Mantenibilidad. En caso de la destrucción de los dispositivos, estos son fáciles de adquirir nuevamente.
f) Velocidad y alcance. Las repercusiones pueden ser instantáneas y llegar a tener efectos en cualquier parte del mundo.[179]

Esto sólo es una aproximación de lo que representa el quinto dominio para los Estados que se encuentran desarrollando instrumentos especializados en materia cibernética para obtener beneficios, y con ello, lograr sus intereses. Visualizar el quinto dominio desde el enfoque de la lucha por el poder, permite entender los fundamentos (ofensivos o defensivos) que utilizan los Estados industrializados y algunos emergentes para ingresar al conflicto en busca de un espacio en el ciberentorno. Además, su estudio genera una mayor comprensión de la complementariedad que ofrece para los otros cuatro dominios en el sentido estratégico y táctico.

Por otra parte, la carencia de regulaciones internacionales y la falta de consenso por definir qué es una ciberarma, una ciberguerra y otros términos que derivan del ciberespacio, permiten que éste espacio virtual sea fortalecido en las agendas, instrumentos y capacidades ofensivas-defensivas de los países en este ámbito.

Es preciso mencionar que se han dado sucesos que se han convertido en un hito para el estudio de la ciberseguridad, pues cada uno representa características peculiares y diferentes. Los casos más emblemáticos son Estonia, *Stuxnet* y *WannaCry*.

3.2 El caso de Estonia

Las cuestiones de la ciberseguridad para Estonia se han fortalecido a partir de los sucesos del 26 de abril del año 2007, fecha en el que fue objetivo de diversos ciberataques.

Todo comenzó porque el gobierno tomó la decisión de trasladar el monumento al Soldado de Bronce, que en el pasado había sido instalado en el Centro de Tallin por las autoridades

[179] Javier López, "La evolución del conflicto hacia un nuevo escenario bélico", en *Monografías del CESEDEN 126*, 2012, p. 140, http://bit.ly/2m3RGUz

de la entonces Unión Soviética.[180] Dicho suceso presentó un gran problema para la población pro rusa, porque para ellos era un símbolo de la victoria de la Unión Soviética sobre los Nazis. Sin embargo, para los estonios, con un determinismo más nacionalista, representaba opresión y ocupación, por lo que era innecesario conservar el monumento.[181]

Tal escenario provocó que se llevarán a cabo una serie de ataques en contra del gobierno y empresas, la forma fue utilizando ciberataques. El objetivo fueron diversas instituciones clave de la República de Estonia, siendo afectados sitios *web* de bancos, medios de prensa, partidos políticos, ministerios e incluso la presidencia y el parlamento.[182]

El tipo de ataque contra los sitios *web* privados y públicos se le denomina «Ataque de Denegación de Servicio» (Distributed Denial of Service, DDoS), el cual, consiste en atacar un objetivo a través del empleo de diversos sistemas, lo que provoca una denegación de servicio a los usuarios que intentan acceder al sistema debido a que se genera una sobrecarga de mensajes entrantes.[183]

Lo que ocurrió es que las plataformas *web* fueron sobrecargadas por la entrada de cantidades masivas de mensajes a los servidores. Una operación normal al día (en ese entonces para los portales), consistía en visitas de entre 1,000 a 1,500; no obstante, se volvió anormal cuando se registraban esas entradas, pero por segundo.

Para determinar quién o quiénes fueron los responsables, se basaron en las direcciones del Protocolo de Internet (IP, por sus siglas en inglés) encontradas y se dieron cuenta de que los ataques provenían de territorio ruso, de modo que algunos funcionarios estonios condenaron a Rusia de ser el responsable de llevar a cabo dichas acciones; sin embargo, la postura del gobierno estonio no expresó que Moscú tuviera injerencia.[184]

[180] Estonia se vuelve independiente de la Unión de Repúblicas Socialistas Soviéticas en el año de 1991. En "Día de la independencia", *Embajada de Estonia en Madrid*, s.f., acceso el 24 de septiembre de 2018 en: http://bit.ly/2kfqhi6

[181] Damien McGuiness, "Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país", *BBC Mundo*, 06 de mayo de 2017, acceso el 26 de septiembre de 2018 en: https://bbc.in/2ktrG4R

[182] Álvaro Fernández, "Estonia, baluarte de la ciberseguridad europea", *El Orden Mundial*, 12 de agosto de 2015, acceso el 26 de septiembre de 2018 en: http://bit.ly/2lJ4D68

[183] Margaret Rouse, "Ataque de Denegación de Servicio (DDoS)", *TechTarget*, s.f., acceso el 26 de septiembre de 2018 en: http://bit.ly/2mb1yvX

[184] Ricardo Martínez, "Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE", *El País*, 18 de mayo de 2007, acceso el 26 de septiembre de 2018 en: http://bit.ly/2lKj3TH

El empleo de *robots* informáticos, denominados *botnets*,[185] hizo posible que el tráfico en los sitios *web* tuviera una sobresaturación, pues muchos ordenadores y dispositivos se encontraban mandando información. Las repercusiones fueron notorias cuando los ciudadanos entraron en pánico al no poder acceder a los servicios bancarios como los cajeros automáticos, y peor aún, cuando los funcionarios no podían comunicarse mediante correos electrónicos.[186]

Las actividades del país en diversos sectores se paralizaron porque no se tenía un plan de acción para afrontar un problema en forma de ataques cibernéticos. La magnitud del malestar ocasionado obligó al gobierno estonio a instrumentar medidas para atender el problema en el corto, mediano y largo plazo.

En ese sentido, el Gobierno estonio creó una Estrategia Nacional de Ciberseguridad en el año 2008, con el objetivo de reducir las vulnerabilidades en el ciberespacio. El plan estaba diseñado para que el Ministerio de Defensa realizara acciones de cooperación con los demás ministerios, y con ello, estableciera un marco de seguridad con base en la Estrategia.[187]

CUADRO 7. MODELO DE LA ESTRATEGIA BASADO EN LA COOPERACIÓN INSTITUCIONAL.[188]

[185] Un *botnet* es «el nombre genérico que denomina a cualquier grupo de PC infectados y controlados por un atacante de forma remota. Generalmente, un hacker o un grupo de ellos crea un botnet usando un malware que infecta a una gran cantidad de máquinas. Los ordenadores son parte del botnet, llamados "bots" o "zombies"». En Dennis Fisher, "Qué es un botnet?", *Kaspersky Lab*, 25 de abril de 2013, acceso el 26 de septiembre de 2018 en: http://bit.ly/2ktBVpM

[186] McGuiness, "Cómo uno de los primeros…".

[187] Javier Candau, "Estrategias nacionales de ciberseguridad. Ciberterrorismo", en *Cuadernos de Estrategia 149*, 2010, p. 289, http://bit.ly/2mb0x77

[188] Elaboración propia con base a datos tomados de Javier Candau, "Estrategias nacionales de ciberseguridad. Ciberterrorismo", en *Cuadernos de Estrategia 149*, 2010, p. 289, http://bit.ly/2mb0x77

Parte esencial de lo desarrollado por el gobierno estonio, radica en los objetivos estratégicos de la estrategia antes mencionada, los cuales se resumen a continuación:

- Aplicar medidas de seguridad de manera gradual en el *Internet*, en los Controles de Supervisión y Adquisición de Datos (SCADA, por sus siglas en inglés), y en las infraestructuras críticas. Además, se deben mejorar las capacidades de detección y respuesta, así como la coordinación entre las agencias.
- Impulsar iniciativas de investigación en ciberseguridad que tengan por objetivo generar conocimiento técnico y permitan la elaboración de normas que mejoren la formación en el ámbito de la seguridad informática.
- Establecer el marco normativo y legal para la protección de sistemas de información e infraestructuras críticas.
- Promover la cooperación internacional para que incentive la creación de acuerdos internacionales y fortalezcan la ciberseguridad, al grado que se puedan condenar el empleo de ciberataques que contravengan los derechos humanos y las libertades democráticas.
- Concientizar a los diferentes sectores en materia de seguridad de la información, pero haciendo especial énfasis en la atención a ciudadanos y a las pequeñas y medianas empresas.[189]

Asimismo, es necesario enfatizar que en el año 2010, se creó la Liga de Ciberdefensa Nacional (*Küberkaitseliit*), derivado de la integración de diversas unidades militares. En este sentido, la finalidad de la liga consiste en defender las infraestructuras de telecomunicaciones de posibles ataques originados en el extranjero.[190]

Su estrategia más reciente se creó en el año 2014, y está diseñada para cubrir tres años. De modo que, se actualizó y modernizó, para adaptarla a las necesidades virtuales de la ciudadanía y gobierno. Su propósito consiste en combatir la ciberdelincuencia, así como proteger las infraestructuras críticas, los servicios vitales y mejorar la capacidad en el ámbito de la defensa nacional.[191]

[189] Ibíd.
[190] Fernández, "Estonia, baluarte de la ciberseguridad…".
[191] James Andrew Lewis, "Experiencias avanzadas en políticas y prácticas de ciberseguridad", *Banco Interamericano de Desarrollo*, 2016, p. 12, http://bit.ly/2lNFG9y

Además, los objetivos de dicha estrategia consisten en:

> Revitalizar un enfoque integral y de todo el gobierno sobre la ciberseguridad;
> Crear un nivel muy alto de competencia y concienciación sobre la ciberseguridad en los organismos, las empresas y el público;
> Fortalecer la regulación para asegurar los sistemas de información;
> Apoyar los esfuerzos para poner en marcha la cooperación internacional en ciberseguridad.[192]

En ese tenor, también incorporó como medida de seguridad el uso de la «nube pública», que tiene como propósito, respaldar en todo momento los servicios electrónicos para que ante un ataque físico o cibernético, las actividades industriales y civiles sigan funcionando a través de una vía alterna. A dicho mecanismo se le denominó «embajadas virtuales».[193]

Parte de los avances en materia de ciberseguridad para Estonia fueron sus aportes para la creación del Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN, en el año 2008. Con base en ello, se han fortalecido las infraestructuras críticas y diversos sectores relacionados. Además, en el ámbito jurídico, se ha procurado establecer el Manual de Tallin[194] para generar fundamentos de Derecho Internacional, que sirvan de base para el establecimiento de un marco que contemple los conflictos que puedan suceder en el ciberespacio. Dicho instrumento adquiere relevancia, porque es un estudio riguroso sobre las implicaciones legales que pueden tener los Estados por el uso de la fuerza a través del ciberentorno.

Por tal motivo, surge la necesidad de crear normas y actualizar la terminología jurídica en el área del Derecho Internacional Público para adecuar los fundamentos que permiten la legítima defensa, de acuerdo al Orden Público Internacional. Si esto es aceptado por una amplia mayoría de Estados, se podrían crear leyes que regulen las acciones ofensivas en el ciberespacio.

La razón por la que Estonia ha dado impulso en temas de seguridad cibernética es porque ha implementado las TIC en diversos sectores con el objetivo de llevar a cabo la transición

[192] Ibíd.
[193] Ibíd., p. 19.
[194] El nombre oficial es Manual de Tallin sobre el Derecho Internacional Aplicable a los Conflictos Armados Cibernéticos y fue elaborado por iniciativa del Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN. En María Pilar Llorens, "Los desafíos del uso de la fuerza en el ciberespacio", *Anuario Mexicano de Derecho Internacional*, vol. XVII, 2017, p. 789, http://bit.ly/2kDbNst

de los servicios de educación, seguridad pública, salud y de gobierno al ámbito digital; de modo que sus sistemas de bases de datos están conectadas a *Internet*. En ese tenor, se puede considerar a Estonia como el primer e-gobierno (gobierno electrónico), donde los ciudadanos pueden ver en tiempo real los gastos del Estado, así como emitir el voto electoral desde sus hogares, pues tienen como mecanismo la identificación digital.[195]

Con base en lo anterior, se creó *X-road* como una herramienta para evitar el robo masivo de datos, de acuerdo al sitio *web e-estonia*, este instrumento es denominado como:

> La columna vertebral de e-estonia. Invisible pero crucial, permite que las diversas bases de datos de servicios electrónicos del sector público y privado del país se conecten y funcionen en armonía.[196]

Estonia ha desarrollado y fortalecido su ciberseguridad en el marco de su transición digital, los ciberataques recibidos y su integración a la OTAN. En ese orden de ideas, el establecimiento de una cultura cibernética más sólida, les ha brindado a sus ciudadanos la experiencia de saber cómo responder ante un escenario como el que se suscitó en el año 2007. De tal manera que, sociedad, sector privado y gobierno, lograron forjar ciberresilencia; con base en ello, el país se ha consolidado como un líder en gobernanza electrónica y en seguridad cibernética.

3.3 El caso de *Stuxnet*

Se trata de uno de los casos más relevantes en los estudios de ciberseguridad, puesto que muchos académicos y expertos han generado análisis y reflexiones sobre si se le debe considerar como un intento de ciberguerra, debido a las características del virus informático y los implicados en el conflicto generado.

El acontecimiento se desarrolló en el año 2010, en el territorio de la República Islámica de Irán. Los objetivos de *Stuxnet* fueron las centrifugadoras que se encargaban del proceso de enriquecimiento de uranio.

Para dimensionar cuáles fueron las características de *Stuxnet*, es necesario especificar qué es un gusano informático. Con base en esto, *Kaspersky Lab* define al gusano como:

---

[195] Muriel Balbi, "Los 7 secretos del país más digital del mundo", *Infobae*, 25 de noviembre de 2017, acceso el 26 de septiembre de 2018 en: http://bit.ly/2m38tqO

[196] "Interoperability services: x-road", *e-estonia*, s.f., acceso el 26 de septiembre de 2018 en: http://bit.ly/2ktCwrw

> Un programa de software malicioso que puede replicarse a sí mismo en ordenadores o a través de redes de ordenadores sin que te des cuenta de que el equipo está infectado… cada copia del virus o gusano informático… puede reproducirse, [de modo que] las infecciones pueden propagarse de forma muy rápida. Existen muchos tipos diferentes de virus y gusanos informáticos,… [que] pueden provocar grandes niveles de destrucción.[197]

La definición nos permite observar dos características principales, que son la propagación y la destrucción. De acuerdo con la anterior definición, existen diferentes niveles en la segunda.

En junio del año 2010, la empresa bielorrusa *VirusBlokAda* detectó la problemática del mal funcionamiento en las centrifugadoras y localizó que un gusano informático, al que se le denominó *Stuxnet*, era el causante de los daños en las máquinas. Lo que más sorprendió a los investigadores fue el grado de sofisticación del virus, pues el código no actuaba de la misma manera que la mayoría de los gusanos informáticos.[198]

Debido a lo anterior, se han generado varios supuestos de cómo fue posible que el virus llegara a los sistemas que controlaban las centrifugadoras, algunos plantean a modo de conjetura que, lo más probable fue que alguien encontró una memoria *Universal Serial Bus* (USB), que contenía el programa malicioso, y al conectarlo a los ordenadores para visualizar la información, se activó el programa y comenzó con su cometido una vez que tuvo acceso a la red interna.

Dicho programa se infiltró en los ordenadores de sistemas industriales que utilizaban como sistema operativo *Windows*. En tanto que los sistemas *SCADA*[199] tienen como función controlar las operaciones de industrias y fábricas, como pueden ser instalaciones militares, o bien, plantas de energía, entre muchas otras.[200]

Es importante señalar que, los virus buscan vulnerabilidades para adentrarse en los sistemas, de modo que *Stuxnet* explotó cuatro a las que se les denomina *Zero-Day.*[201] Los

---

[197] "Virus y gusanos informáticos", *Kaspersky Lab*, s.f., acceso el 26 de septiembre de 2018 en: http://bit.ly/2lNGN9e

[198] Gema Sánchez, "La ciberguerra: los casos de Stuxnet y Anonymous", *DERECOM*, n. 11, 2012, p. 129, http://bit.ly/2kDaeKY

[199] Véase p. 76.

[200] Abraham González, "El ciberespacio en la guerra moderna", *ININVESTAM.* Documento de Análisis, DA. 21/18, 2018, p. 11, http://bit.ly/2keaoII

[201] *Welivesecurity* denomina *Zero-Day* como: «Una nueva vulnerabilidad para la cual no se crearon parches o revisiones, y que se emplea para llevar a cabo un ataque. El nombre 0-day se debe a que aún no existe ninguna revisión para mitigar

efectos del virus permitieron reprogramar los sistemas de las maquinas al alterar su funcionamiento.[202] Cuando se pasaron las barreras, el código tenía como propósitos buscar dos microchips, cuyo trabajo consistía en controlar la velocidad de rotación de los motores de las máquinas, de manera específica, los que tenían velocidades de entre 807 Hz y 1,210 Hz.[203]

Las especificaciones del código consistían en alterar las funciones de las máquinas, cambiando los tiempos de rotación; esto hizo posible que durante 15 minutos giraran a una velocidad muy rápida, pero después, por un lapso de 50 minutos, las desaceleró.[204] Al modificar esto bruscamente, la operación normal de las centrifugadoras se dañó debido a la inestabilidad en su funcionamiento, haciéndolas inservibles.

Por lo tanto, una de las potencialidades de este virus, es lo avanzado que estaba en su programación, pues su función no consistía en sólo alterar la velocidad en las rotaciones de las centrifugadoras, también tenía como propósito mostrar información errónea. En esa tesitura, los datos de la operatividad de las máquinas mostraban un funcionamiento normal,[205] aunque en realidad, su actividad estaba corrompida por el virus. Por otra parte, *Stuxnet* no perjudicaba a los ordenadores que no cumplían con los requisitos anteriormente mencionados, pese a ello, se estima que tomó el control de 1,000 máquinas y causó su inoperatividad al destruirlas.[206] Esto hizo posible que fuera difícil detectar al virus, toda vez que no se comportaba como los demás.

Las repercusiones fueron notorias para Irán al mermar su proceso de enriquecimiento de uranio, pues a causa del mal funcionamiento de las centrifugadoras, sus operaciones se detuvieron debido a las acciones del gusano informático especializado que, causó estragos

---

el aprovechamiento de la vulnerabilidad. Estas a veces se usan junto a los troyanos, rootkits, virus, gusanos y otros tipos de malware, para ayudarlos a propagarse e infectar más equipos». Aunado a lo anterior, define vulnerabilidad como: «El punto débil que puede causar que los programas se comporten de manera extraña. Si alguien descubre la presencia de una vulnerabilidad, puede utilizar ese comportamiento extraño para crear una falla por donde los atacantes pueden ingresar y lograr que se ejecute su propio código malicioso». En Lisa Myers, "Security terms explained: What does Zero Day mean?", *Welivesecurity by eset*, 11 de febrero de 2015, acceso el 26 de septiembre de 2018 en: http://bit.ly/2kqZqQh

[202] Robert Lipovsky, "A siete años de Stuxnet, los sistemas industriales están nuevamente en la mira", *Welivesecurity by eset*, 20 de junio de 2017, acceso el 26 de septiembre de 2018 en: http://bit.ly/2lPJqaz

[203] González, "El ciberespacio en la guerra…", p. 12.

[204] "El virus que tomó control de mil máquinas y les ordenó autodestruirse", *BBC Mundo*, 11 de octubre de 2015, acceso el 26 de septiembre de 2018 en: https://bbc.in/2m39jns

[205] González, "El ciberespacio en la guerra…", p. 13.

[206] "El virus que tomó control…".

reales en el aspecto físico, específicamente en infraestructuras críticas para Teherán. En ese sentido, y para hacer más claro lo anterior, es indispensable mencionar el rasgo distintivo de lo que representan los Sistemas Físico-Cibernéticos (SFC), en un entorno de ciberseguridad.

Un SFC puede ser descrito por su utilización, es decir, son sistemas que emplean los recursos de la red y los ordenadores para realizar tareas en el mundo físico, ya sean actividades industriales, o bien, las comunicaciones, los sistemas de aguas, entre muchos otros. En ese tenor, González específica que:

> Un SFC está diseñado para tener efectos cinéticos, en el "mundo real" y el funcionamiento de un SFC es controlado por un sistema de computadoras que… funciona a partir de un código de computadora…, el sistema computacional está operando en el ciberespacio, y dada la interconectividad de dichos sistemas computacionales con los SFC que éstos controlan, es posible manipular cibernéticamente dichos sistemas computacionales para utilizar los SFC con propósitos distintos para los que fueron diseñados.[207]

Al analizar lo dicho por González, entendemos de qué manera un código puede arremeter contra objetos del mundo real que tengan conexión a un sistema de computadora, tal es el caso de las centrifugadoras de Irán que fueron modificadas y manipuladas para que se autodestruyeran con las ordenes que emitían los códigos de *Stuxnet*.

Visto de esta manera, la sofisticación que tenía es muy diferente a los gusanos comunes, de modo que alguien tuvo que haber empleado mucho tiempo y recursos para crear un programa malicioso de ese tipo. Algunos consideran que fue desarrollado por Estados Unidos e Israel para mermar y detener la producción de uranio por parte de Irán; sin embargo, no se puede comprobar a ciencia cierta si esto es verdadero, por lo que sólo se puede establecer como conjetura ante las cuestiones geopolíticas de la zona.

Lo que sí se puede corroborar es la ofensiva especializada de dicho virus contra programas específicos; en tal sentido, Sánchez menciona que «ya es considerado como la mejor arma cibernética jamás creada, al haber dejado fuera de combate a un 20% de las centrifugadoras».[208]

[207] González, "El ciberespacio en la guerra…", p. 10.
[208] Sánchez, "La ciberguerra: los casos…", p. 130.

Este caso permite comprender los efectos negativos que puede ocasionar un ataque cibernético en objetos físicos, sobre todo en las infraestructuras industriales de algún país. La naturaleza de los implicados en el conflicto sugiere que la disputa puede ser entre los Estados anteriormente mencionados por la coyuntura de ese entonces, y también por la situación geopolítica y de seguridad que algunos países consideran de gran importancia, lo que supondría el comienzo de la creación de armas cibernéticas con códigos especializados para lograr objetivos estratégicos.

3.4 El mundo después de *WannaCry ransomware attack*

El ciberataque *WannaCry* se desarrolló en mayo del año 2017, cuando a escala global se comenzaron a reportar noticias de un virus informático que estaba causando daños a instituciones, empresas e individuos de diversos países (Rusia, España, México, Estados Unidos de América, entre muchos otros).

Se trató de un virus tipo *ransomware*, el cual *Kaspersky Lab* define como «un tipo de *ciberware* diseñado para obtener dinero de una víctima. A menudo, el *ransomware* exige un pago para deshacer los cambios que el virus troyano haya realizado en la computadora de la víctima. Estos cambios pueden incluir: cifrar datos almacenados en el disco de la víctima, para que ésta no pueda acceder a la información, y bloquear el acceso normal al sistema de la víctima».[209]

Panda Security lo define como:

> […] un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados. El virus lanza una ventana emergente en la que nos pide el pago de un rescate, dicho pago se hace generalmente en moneda virtual (*bitcoins* por ejemplo).[210]

Dichas definiciones expresan, de manera precisa, lo que hizo este virus. Cifró los archivos de los ordenadores donde se propagó. Se estima que el ciberataque afectó a unos 200,000

[209] "Ransomware: definición, prevención y eliminación", *Kaspersky Lab*, s.f., acceso el 27 de septiembre de 2018 en: http://bit.ly/2m39xei

[210] "¿Qué es un Ransomware?", *Panda Security*, 15 de noviembre de 2013, acceso el 27 de septiembre de 2018 en: http://bit.ly/2lK13Zs

mil usuarios en 150 países,[211] dicha cifra resulta enorme por la cantidad de equipos infectados. Asimismo, las pérdidas económicas que sufrieron las personas y las empresas a nivel internacional son considerables, porque el código malicioso solicitaba un pago de entre 300 a 500 dólares en *bitcoins* para que pudieran acceder a los archivos.

El Reino Unido de la Gran Bretaña e Irlanda del Norte, tuvo complicaciones en sus servicios de salud al no poder acceder a los datos de los pacientes, debido a que los archivos se encontraban cifrados. En ese sentido, las afectaciones se extendieron en Inglaterra y Escocia, por lo que tuvieron que suspender ciertas actividades laborales.[212]

Por otra parte, la empresa *Renault* tuvo afectaciones en la producción de vehículos en sus fábricas en Francia, de modo que también detuvieron sus actividades por los problemas que causaba el virus.[213]

Los dos ejemplos anteriores permiten dimensionar dos sectores que pueden ser considerados críticos; el primero de ellos es el de la salud, que como bien se especificó, el virus hizo posible que no se permitiera el acceso a los datos de pacientes, esto es vital porque puede causar el deceso de personas que se encuentran en un estado grave de salud. El segundo se refiere a las actividades de un sector que puede ser considerado estratégico para diversos Estados de acuerdo a sus intereses industriales y comerciales, de modo que si se detiene la producción, puede ocasionar pérdidas económicas significativas respecto a otros competidores.

De acuerdo con Blanco, el ciberataque sucedió porque la Agencia de Seguridad Nacional de Estados Unidos (NSA, por sus siglas en inglés), fue *hackeada* por el grupo denominado *The Shadow Brokers*.

Dicho grupo sustrajo información y también robó herramientas cibernéticas de espionaje, las cuales, después de ser utilizadas y probar sus funciones, las publicaron en línea.[214] Una de las herramientas sustraídas a la NSA fue utilizado en *WannaCry*, dicho instrumento se refiere

[211] "El ciberataque de escala mundial y 'dimensión nunca antes vista' que afectó a instituciones y empresas de unos 15 países", *BBC Mundo*, 13 de mayo de 2017, acceso el 27 de septiembre de 2018 en: https://bbc.in/2keaMa8
[212] Ibíd.
[213] Ibíd.
[214] Daniel Blanco, "A esta velocidad corre el cronómetro de pérdidas económicas por el ciberataque global", *El Financiero*, 14 de mayo de 2017, acceso el 27 de septiembre de 2018 en: http://bit.ly/2kGIlxt

al uso de *EternalBlue*,[215] el cual es un *exploit*[216] que posibilita la carga de códigos maliciosos a través del empleo de *DoublePulsar*.[217]

Esto sucede cuando el e*xploit* concede los permisos necesarios para que los programas infectados se ejecuten sin que el usuario pueda hacer algo al respecto. De esa manera, cuando el código malicioso accedió a los ordenadores, la siguiente fase consistió en cifrar los archivos y activó la ventana emergente de requerimiento de pago para acceder nuevamente a los datos.

Cabe destacar que existen *exploits* conocidos y desconocidos, los primeros son todos aquellos de los que ya se tiene conocimiento, por lo tanto se pueden tomar medidas al respecto. En lo que refiere a los segundos, se les denomina z*ero-days* porque se utilizan sobre vulnerabilidades que todavía no han sido reportadas, por lo que no se tiene referencia de ellos y suponen una grave amenaza.[218]

WannaCry logró dañar a diversos países, aunque algunos tuvieron más afectaciones que otros. Rusia fue el más perjudicado con un porcentaje del 33.64%; el segundo fue Vietnam con un 12.45%, y en tercer lugar se posicionó India con un 6.95%. En lo que respecta a la región de América Latina, México, Colombia y Brasil fueron los más perjudicados.[219]

La arquitectura de este virus, sin duda, es muy diferente al tipo de ataque contra los sitios *web* de Estonia y las infraestructuras críticas en Irán, puesto que éstos tenían como objetivo una acción específica; sin embargo, las acciones de *WannaCry* consisten en atacar a empresas, instituciones e individuos. De esta manera, se puede inferir que su objetivo es general, siempre y cuando acceda a los ordenadores para requerir un pago.

---

[215] «EternalBlue es una vulnerabilidad en los sistemas Windows que tienen versiones desactualizadas del servicio de uso compartido de archivos e impresoras». En "Cómo actualizar Windows para reparar la vulnerabilidad EternalBlue y evitar el ataque DoublePulsar", *AVG,* s.f., acceso el 27 de septiembre de 2018 en: http://bit.ly/2kfXOJ2

[216] *Welivesecurity* define *exploit* como: «…programa malicioso que se aprovecha de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema, de forma que un atacante podría usarla en su beneficio». En Josep Albors, "¿Sabes qué es un exploit y cómo funciona?", *Welivesecurity*, 09 de octubre de 2014, acceso el 27 de septiembre de 2018 en: http://bit.ly/2kGmjiH

[217] DoublePulsar es una puerta trasera que se utiliza para inyectar y ejecutar códigos maliciosos en un sistema infectado, de modo que EternalBlue lo instala y lo utiliza. En Bhat Shakeel, "DoublePulsar-A very sophisticated Payload for Windows", *Secpod*, 01 de junio de 2017, acceso el 27 de septiembre de 2018 en: http://bit.ly/2lK1OSi

[218] Albors, "¿Sabes qué es un exploit…".

[219] "A un año de WannaCry el exploit EternalBlue sigue siendo un vector de infección", *Kaspersky Lab*, 11 de mayo de 2018, acceso el 27 de septiembre de 2018 en: http://bit.ly/2kDdeHn

En ese sentido, Martínez menciona que este virus se puede dividir en tres elementos: por su alcance, por la arquitectura del ataque y porque fue creada por una institución gubernamental. El primero se refiere a que las afectaciones iniciaron en Reino Unido y España; pero, de manera posterior, se esparcieron globalmente. En lo referente a la arquitectura, se establece que *WannaCry* está compuesto por un gusano informático y un *ransomware*; y el tercero argumenta que dicho código malicioso fue una creación de la NSA[220], lo cual puede ser cierto si se toma en cuenta la arquitectura del virus, así como las revelaciones del grupo de *hackers The Shadow Brokers*.

En contraposición, Estados Unidos atribuyó la creación de *WannaCry* a Corea del Norte, enfatizando que las presiones comerciales que se han impuesto por el desarrollo de armas nucleares, ha impulsado al Gobierno de Pyongyang a desarrollar armamento cibernético para promover sus intereses.[221]

En ese tenor, esto demuestra que en el ámbito cibernético, cualquier acción en forma de ciberataque, es difícil de rastrear, pues la característica del anonimato evidencia que no siempre se puede identificar al responsable directo del desarrollo de códigos sofisticados. De modo que, en el marco de la Cuarta Revolución Industrial, se debe destacar como un factor de riesgo la dependencia tecnológica, puesto que una débil seguridad cibernética puede contribuir a que los efectos negativos de un código malicioso como *WannaCry*, se multipliquen rápidamente.

La sofisticación de este virus, implica un enorme desafío para la seguridad nacional e internacional, debido a que una agencia estatal fue participe en su creación. A su vez, el impacto que tuvo fue global, pues perjudicó a diversos países de maneras muy variadas y particulares.

Para enfatizar lo anterior, es prudente citar lo dicho por el Director del Equipo de Investigación y Análisis de *Kaspersky Lab* en Latinoamérica, Dmitry Bestuzhev, el cual señala que:

[220] Francisco Martínez, "La vida después de wannacry", *Dirección General de Cómputo y de Tecnologías de Información y Comunicación, UNAM*, s.f., acceso el 27 de septiembre de 2018 en: http://bit.ly/2m6sMDO

[221] Andy Sharp y David Tweed, "Estados Unidos culpa a Norcorea por ataque 'cobarde' de WannaCry", *El Financiero*, 19 de diciembre de 2017, acceso el 27 de septiembre de 2018 en: http://bit.ly/2mc2RLf

> El mundo ha caído en una carrera de armamento cibernético… [tanto] de armamento defensivo… [como] de armamento ofensivo y en este afán… los países buscan encontrar… *exploits* para estas vulnerabilidades, y las ocultan por el máximo tiempo posible porque mientras se desconozca que existe tal vulnerabilidad con su *exploit*, entonces el arma funciona.[222]

Su argumento es válido porque es lo que sucedió con *EternalBlue*, aprovecharon las vulnerabilidades de muchos ordenadores, y con ello, se logró evidenciar tres cosas: el primero es el rol que tienen las instituciones estratégicas de los Estados en la creación de armas cibernéticas, lo segundo radica en el desconocimiento de dichos instrumentos por parte de algunos países, y tercero, que por todo lo anterior, las repercusiones son globales. Por lo tanto, es evidente que en un mundo interdependiente e interconectado, el criterio de las fronteras ha sido rebasado ante la nueva dinámica que representa el ciberespacio.

Los tres casos de ciberataques, descritos en este capítulo, adquieren un matiz relevante al exponer que en lo digital existen muchas vulnerabilidades que pueden ser aprovechadas no sólo por Estados, sino también por grupos delictivos de muy diferentes maneras. El caso de Estonia permite observar de qué manera se puede paralizar un país, si no se tiene un plan de acción en materia de ciberseguridad. En lo que respecta a *Stuxnet*, la evidencia muestra que lo cibernético sí puede tener impacto en el mundo real, precisamente en las infraestructuras críticas con la aplicación de códigos altamente especializados. Por último, el caso de *WannaCry* ejemplifica la fragilidad que existe de manera global, por la falta de estrategias, políticas y ordenamientos jurídicos en el tema de la ciberseguridad.

[222] Blanco, "A esta velocidad corre…".

CAPÍTULO 4

LA SITUACIÓN DE MÉXICO EN MATERIA DE CIBERSEGURIDAD

El asunto del ciberespacio ha ido cobrando gran dinamismo en los asuntos internacionales, regionales y nacionales, por lo que algunos países y organizaciones lo desarrollan desde un enfoque económico, jurídico, político, social o militar para fortalecer sus capacidades en materia de ciberseguridad y atenuar la problemática de la ciberdelincuencia.

Analizar el caso de México y el tema de la ciberseguridad permitirá observar cuáles han sido los efectos negativos para el país ante los ciberataques que ha padecido. Por otra parte, se examinará el rol de las instituciones encargadas de la seguridad y defensa, así como el sistema financiero y las infraestructuras críticas en el ámbito del ciberespacio.

4.1 Daños por ciberataques en México

Los ataques cibernéticos tienen un impacto global debido a que pueden ser llevados a cabo desde cualquier parte del planeta, por las características que se han explicado en los capítulos anteriores. De modo que, la preocupación por la materialización de ciberataques ha aumentado al punto de que el informe anual del Foro Económico Mundial, *Global Risk Report*, los considerara como uno de los principales riesgos que tienen más probabilidad de que sucedan en el corto, mediano y largo plazo.

Para el reporte del año 2018, se enmarcan cinco riesgos, el primero de ellos se refiere al clima extremo; el segundo a desastres naturales; el tercero a los ataques cibernéticos; el cuarto al fraude o robo de datos, y el quinto a la adaptación al cambio climático.[223]

Los ciberataques y el robo de datos figuran entre los 5 principales riesgos que deben ser atendidos, puesto que son una realidad que afecta a la mayor parte de las naciones. A medida de que los impactos negativos aumenten en el ciberespacio, es muy probable que diversos Estados lo consideren como un factor de riesgo en el mediano y largo plazo.

En el caso de México el asunto se torna complejo por la cantidad de intrusiones cibernéticas que se han llevado a cabo en el ciberespacio. De acuerdo al diario alemán *Der Spiegel*, la Agencia de Seguridad Nacional de los Estados Unidos (NSA, por sus siglas en inglés),

[223] Alex Gray, "Estos son los mayores riesgos que enfrenta el mundo", *World Economic Forum*, 17 de enero de 2018, acceso el 29 de septiembre de 2018 en: http://bit.ly/2kaOVQN

accedió a los correos electrónicos del entonces presidente Felipe Calderón y su gabinete. En el año 2012, también se vulneró el correo del ex presidente electo Enrique Peña Nieto y en el año 2013, el portal de la Secretaría de la Defensa Nacional (SEDENA) fue vulnerado por el grupo *Anonymous.*[224]

En la administración del ex presidente Enrique Peña Nieto, se dio un impulso a la implementación de Tecnologías de la Información y la Comunicación, especialmente, las que tienen como propósito aumentar la cobertura de banda ancha y de acceso a *Internet*. En este sentido, *Internet* es utilizada por más de 3,600 millones de personas en todo el mundo, pero para el caso de México, existen 65 millones de cibernautas, lo que representa un 59% de las personas que habitan el país.[225]

Aunado a lo anterior, las estimaciones de *Symantec* sugieren que 40% de esas personas han sido víctimas de algún crimen en el ciberespacio; de ese porcentaje, un 58% de los delitos tienen una categoría de suplantación y robo de identidad, mientras que un 17% representa los fraudes y un 15% *hackeo*.[226]

Un problema general es la falta de cultura en ciberseguridad,[227] ya que gran parte de la población no tiene los conocimientos necesarios para llevar a cabo una efectiva protección de sus datos personales. Además, no tienen instalados antivirus que estén adaptados a las actividades que desarrollan en sus ordenadores. Complementando esta idea, un estudio de la consultora *PricewaterhouseCoopers* (PwC), revela que 43% de las empresas mexicanas han sido víctimas de perdida de información, y un 86% no tiene en consideración las

[224] Javier Tejado, "México reprobado en ciberseguridad", *El Universal*, 28 de julio de 2015, acceso el 29 de septiembre de 2018 en: http://bit.ly/2lL2iaP

[225] Patricia Trujillo, "El ciberespacio, recurso y responsabilidad de los Estados", *ININVESTAM*, México, 2017, p. 2, http://bit.ly/2m5hyPT

[226] Javier Arreola, "Ciberseguridad (casi) a prueba del enemigo 'invisible'", *Forbes México*, 20 de mayo de 2016, acceso el 29 de septiembre de 2018 en: http://bit.ly/2ma7WUb

[227] Con cultura en ciberseguridad me refiero a los conocimientos básicos o necesarios para llevar a cabo acciones seguras de comunicación, almacenamiento y difusión de información o datos a través del uso de redes informáticas. En tal sentido, conocer y saber sobre protocolos de seguridad en los dispositivos electrónicos (computadoras, móviles y equipos inteligentes) permitiría navegar sin riesgos en el ciberespacio. La siguiente definición es la que aporta la Estrategia Nacional de Ciberseguridad que desarrolló México, la cual podrá ser visualizada en capítulos posteriores, pero para efectos de esta investigación se precisa la siguiente definición: «…conjunto de valores, principios y acciones en materia de concientización, educación y formación, que se llevan a cabo por la sociedad, academia, sector privado e instituciones públicas, que inciden en la forma de interactuar en el ciberespacio de forma armónica, confiable y como factor de desarrollo sostenible». "Estrategia Nacional de Ciberseguridad", gob.mx, 2017, p. 19, http://bit.ly/2ktuizH

consecuencias por el hurto de la misma.[228] En tal sentido, son diversas las pequeñas y grandes compañías que sufren ataques cibernéticos; no obstante, es preciso señalar que en México, el objetivo de los delincuentes es el sistema financiero o cualquier otro actor que forme parte de dicho sistema (como pueden ser bancos, casas de cambio e instituciones gubernamentales), las principales razones son las altas cifras de capital que poseen, así como la información de los clientes que forman parte de sus listas.

Conforme hay más avances tecnológicos en los dispositivos y ordenadores, mayor es el riesgo de padecer algún problema cibernético en materia de ciberdelincuencia. Para ilustrar esto, en el año 2015, Mario Di Costanzo, Presidente de la Comisión Nacional para la Protección y Defensa de Usuarios de Servicios Financieros (CONDUSEF), precisó que la cifra por robos de identidad ascendió a 30 mil.[229] La situación por ciberataques en los años posteriores no ha mejorado, puesto que siguen existiendo grandes pérdidas de datos, causando daños de carácter económico. Ejemplo de esto lo dio a conocer la misma Comisión en el año 2015, cuando estimaron que los usuarios que utilizan servicios financieros, perdieron en conjunto, alrededor de 150 millones de pesos.[230]

En el ámbito político-institucional, México también tuvo consecuencias a causa de acciones de ciberespionaje contra secretarías de Estado. La información sobre espionaje cibernético, fue revelada por el grupo de *hackers The Shadow Brokers*, los cuales, publicaron las listas en las que se visualizan 306 dominios y 352 direcciones IP de 49 países que la NSA de los Estados Unidos estuvo vigilando, y en cuyas datos destacan México, Rusia, China, India y Suecia.[231]

Las instituciones mexicanas que aparecen en los registros son la Secretaría de Gobernación, de Desarrollo Social y la Universidad Nacional Autónoma de México.[232] Dichos problemas,

[228] Diana Nava, "¿Qué retos tiene México ante un ciberataque?", *El Financiero*, 19 de mayo de 2017, acceso el 29 de septiembre de 2018 en: http://bit.ly/2kDdZjH
[229] Carmen Álvarez, "México, más vulnerable a ciberataques", *Excélsior*, 26 de agosto de 2016, acceso el 29 de septiembre de 2018 en: http://bit.ly/2ktG9xG
[230] Ibíd.
[231] Paul Lara, "Estados Unidos hackeó a Segob, Sedesol y UNAM", *Imagen Digital*, 01 de noviembre de 2016, acceso el 29 de septiembre de 2018 en: http://bit.ly/2kfZlPi
[232] Ibíd.

representan un asunto crítico por el tipo de información a la que tuvieron acceso y también porque son dependencias estratégicas para Estado mexicano.

En el foro denominado «HablemosdeCiberseguridad», organizado por la empresa *Microsoft*, se dieron a conocer los resultados del año 2015, mediante la medición del Índice Mundial de Ciberseguridad,[233] en el que le otorgaron a México una calificación del 25% en seguridad cibernética. Aunado a ello, en el aspecto cultural, le asignaron una calificación de 2, en una escala donde 1 es lo más bajo y 5 lo más alto.[234] Esto significa que existe un problema general, puesto que las empresas, los individuos y las instituciones son vulnerables ante diferentes tipos de actores que tengan como objetivo, obtener beneficios de distinta índole a través del uso del ciberespacio.

El factor cultural sigue estando presente, pues entre menos conocimientos tengan las personas sobre los riesgos en el ciberespacio, es posible que se materialicen diversos tipos de ciberataques. Por otra parte, en el ámbito jurídico no se ha trabajado lo suficiente, porque aún falta desarrollar leyes que castiguen los distintos tipos de delincuencia en el ciberespacio.

Complementado la idea anterior, la OEA junto con la empresa *Symantec*, desarrollaron un reporte en el año 2014 denominado «Tendencias de Seguridad Cibernética en América Latina y el Caribe», en el que establecen, el problema del aspecto legislativo en México en dicha materia. A saber:

> [Es evidente el]… gran número de impedimentos para reducir el delito cibernético y aumentar la seguridad cibernética en México. Uno de ellos es la constante falta de legislación que permita a las entidades policiales actuar en forma inmediata para enfrentar las amenazas a la seguridad y los delitos cibernéticos. La capacidad limitada de las entidades policiales para actuar en muchas instancias debilita las investigaciones, perpetúa la sensación de impunidad entre los grupos criminales organizados y les permite implementar las últimas tecnologías y técnicas para cometer delitos. El otro gran impedimento identificado es la constante falta de conciencia entre la población general sobre seguridad cibernética, incluidos riesgos y prácticas recomendadas.[235]

[233] Cabe destacar que dicho índice es distinto al que elabora la Unión Internacional de Telecomunicaciones.
[234] Omar Ortega, "¿Qué tan protegido está México ante la ciberdelincuencia?", *El Financiero*, 30 de mayo de 2017, acceso el 29 de septiembre de 2018 en: http://bit.ly/2kE3L2w
[235] "Tendencias de Seguridad Cibernética en América Latina y el Caribe 2014", *Organización de los Estados Americanos/Symantec*, 2014, p. 68, https://symc.ly/2lKmdXz

De acuerdo al Índice Mundial de Ciberseguridad (IMC), desarrollado por la Unión Internacional de Telecomunicaciones, en el año 2017, México se posicionaba en el lugar número tres del continente, por debajo de Estados Unidos y Canadá. Respecto a Estados Unidos tenía una diferencia de 0.25 puntos, y con Canadá de 0.15 puntos.[236]

De esta manera, la calificación de México era de 0.66; sin embargo, a nivel mundial México ocupó la posición número 28 respecto a la medición del año 2017.[237] Para el año 2018, México descendió 35 lugares según reporta el IMC, de modo que ahora se encuentra en la posición número 63.[238]

CUADRO 8. LOS TRES PAÍSES CON MEJOR POSICIÓN EN CIBERSEGURIDAD EN AMÉRICA PARA EL AÑO 2017.[239]

País	Calificación	Aspecto legal	Aspecto técnico	Aspecto Organizacional	Capacidad de Construir	Cooperación
Estados Unidos	0.91	1	0.96	0.92	1	0.73
Canadá	0.81	0.94	0.93	0.71	0.82	0.70
México	0.66	0.91	0.89	0.48	0.68	0.34

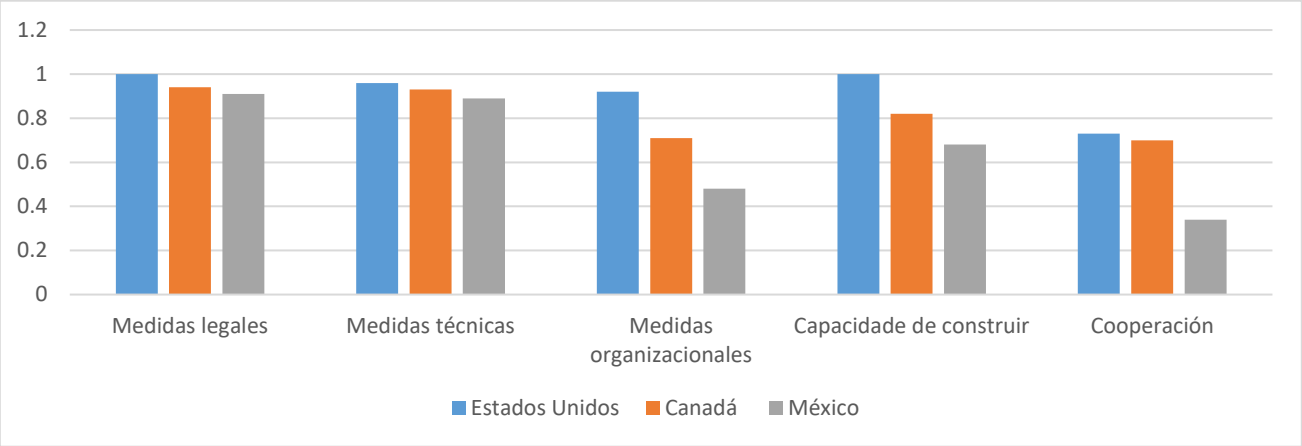
El cuadro 8 expresa que México estaba entre los tres mejores del continente, no obstante a nivel internacional se encontraba en la posición número 28. Esto quiere decir que en la evaluación continental su posición era relativamente buena, pero si lo contrastamos con las calificaciones a nivel internacional, México se ubicaba diecinueve lugares por debajo de Canadá y veintiséis de Estados Unidos.

En 2017, la primera posición la tenía Singapur con una evaluación de 0.92, mientras que el último puesto lo tenía Guinea Ecuatorial con 0.00 y ocupaba el lugar número 164.[240] No

[236] "Global Cybersecurity Index 2017", p. 28.
[237] Ibíd.
[238] "Global Cybersecurity Index 2018", *International Telecommunication Union*, 2019, http://bit.ly/2lHoMts
[239] "Global Cybersecurity Index 2017", *International Telecommunication Union*, 2017, http://bit.ly/2kD8GRj
[240] Ibíd.

obstante, para 2018, quien lidera es Reino Unido de la Gran Bretaña e Irlanda del Norte con una calificación de 0.93 y la última posición la tiene Maldivas con 0.004.[241]

CUADRO 9. COMPARÁCIÓN DE LOS TRES PAÍSES MEJOR SITUADOS EN CIBERSEGURIDAD EN AMÉRICA DEL NORTE PARA EL AÑO 2017.[242]



La información presentada en los gráficos anteriores nos muestra la diferencia existente entre los países que conforman la región de América del Norte, pues el IMC los calificó como los mejores del continente en materia de ciberseguridad, considerando los cinco parámetros de medición. Si observamos el cuadro 9, podemos identificar de mejor manera que, México tiene un nivel bajo respecto a Estados Unidos y Canadá en el área organizacional, de cooperación y en la capacidad de construir.

Sin embargo, para el año 2018, México a nivel continental ya no se encuentra en dicho puesto, toda vez que descendió 35 lugares; en su lugar se encuentra Uruguay con una calificación de 0.681 y ocupa la posición 51 mientras que México tiene 0.629 y está en el puesto 63.

De acuerdo al informe del año 2017, en el ámbito legal y técnico, México parece tener un nivel óptimo, no obstante, si en el aspecto operativo se encuentra bajo, su capacidad de respuesta será baja o nula ante eventuales ataque cibernéticos. Para contrastar esto, de acuerdo a cifras de *SonicWall*, en marzo del año 2018, México se posicionó como el tercer país con mayor índice de ataques cibernéticos a nivel mundial; en este sentido, las

[241] "Global Cybersecurity Index 2018", p. 67-68.
[242] Elaboración propia con datos del gráfico anterior.

amenazas por *malware* se incrementaron un 215%, a diferencia del promedio a nivel global, que es de 102%, de modo que dicha amenaza perjudica a la sociedad en general. [243]

Esto evidencia que los riesgos y vulnerabilidades por ciberataques en el país, siguen en aumento. Si bien el Índice Mundial de Ciberseguridad (IMC) le otorgó a nivel continental la posición número 3 en el año 2017, a nivel internacional, para el 2018, descender 35 lugares demuestra que a México sí le hace falta seguir trabajando en dicho tópico, por lo que se vuelve indispensable fortalecer y subsanar las áreas en las que tiene una baja capacidad, que en este caso sería el aspecto operativo y de repuesta. En esa tesitura, también es necesario seguir trabajando en el ámbito legal y técnico, puesto que son áreas que no deben pasar desapercibidas sólo por tener un buen desempeño, según lo demostró el IMC.

Por otra parte, en mayo del año 2018, se registró un ataque cibernético ante el sistema financiero. El objetivo fue el Sistema de Pagos Electrónicos Interbancarios (SPEI), el cual, es regulado por el Banco de México. Los costos económicos por el ciberataque ascendieron a los 300 millones de pesos,[244] lo cual es una cifra alta en daños.

Las consecuencias directas de este ataque, fueron las siguientes:

- Bancos afectados: Citibanamex, Banorte y Banjercito registraron sustracciones de dinero no autorizadas;
- no se logró identificar a los responsables del delito, aunque, se piensa que fueron especialistas en operaciones cibernéticas, y;
- se suscitó un retraso en las transferencias bancarias porque se tuvo que utilizar un sistema alterno por las afectaciones al SPEI.[245]

Para castigar a los responsables, primero es necesario localizarlos, y para ello se requiere del trabajo coordinado entre instituciones. En ese sentido, el Banco de México puso a disposición de la entonces Procuraduría General de la República los hechos ocurridos para que se abriera una investigación. Al recibir el caso, éste fue asignado a la Unidad de

[243] Omar Ortega, "México, la tercera nación con más ciberataques en el mundo", *El Financiero*, 30 de julio de 2018, acceso el 29 de septiembre de 2018 en: http://bit.ly/2mbhzC4

[244] "Puntos importantes sobre la situación actual del SPEI", *Banco de México*, 22 de mayo de 2018, acceso el 29 de septiembre de 2018 en: http://bit.ly/2m3crjc

[245] "México: el ciberataque "sin precedentes" a los bancos del país que causó pérdidas millonarias", *BBC Mundo*, 15 de mayo de 2018, acceso el 29 de septiembre de 2018 en: https://bbc.in/2kajgyT

Investigaciones Cibernéticas y Operaciones Tecnológicas (UICOT), de la Agencia de Investigación Criminal (AIC).[246] La investigación tiene como propósito identificar las vulnerabilidades, los vectores de ataque y el *modus operandi* de los responsables para generar un registro de lo sucedido.[247]

La situación de México es compleja porque a partir del año 2012, los ciberataques que han ocurrido, tienen impacto en diversos ámbitos; los ciberdelincuentes no sólo tienen como objetivo el hurto de información a las personas, también lo ha sido el sistema financiero, por los grandes beneficios económicos que pueden adquirir. Por otra parte, las acciones de ciberespionaje se llevan a cabo contra políticos, instituciones y dependencias gubernamentales que son objeto de interés para gobiernos de otros países, lo que supone un grave riesgo por el tipo de información que puede ser sustraída.

En consecuencia, se debe hacer énfasis de que la falta de cultura en ciberseguridad perjudica el desarrollo de diversos sectores que emplean las TIC para realizar sus actividades. Los efectos negativos son grandes y crecientes, puesto que México tiene las condiciones ideales para que los delincuentes lleven a cabo actos ilícitos en el ciberespacio.

Sin duda, los ciberataques son un problema creciente que, a medida que surja un mayor dinamismo tecnológico y económico, hará que se requiera de mejores niveles en seguridad cibernética y será necesario tener conocimientos óptimos de los riesgos existentes en el ciberespacio, toda vez que hay un gran desconocimiento a nivel general. Los daños son evidentes y pueden aumentar si no se trabaja en acciones de ciberseguridad en el corto, mediano y largo plazo. El sistema financiero mexicano es un sector que está en la mira de diversos actores, no obstante, también existen otros que, en la transición tecnológica, pueden implementar las innovaciones de la Cuarta Revolución Industrial, lo que presenta ventajas, pero también efectos negativos si no se fortalecen los esquemas de ciberseguridad.

[246] Manuel Espino, "PGR tiene distintas líneas de investigación sobre ataque cibernético", *El Universal*, 16 de mayo de 2018, acceso el 29 de septiembre de 2018 en: http://bit.ly/2ktv4wB
[247] Ibíd.

4.2 El rol de las instituciones estratégicas

Toda institución tiene una función a desempeñar, además de un objetivo, una misión y una visión. Hay algunas que se dedican a la atención ciudadana y tienen un enfoque económico, social, político o académico; sin embargo, otras adquieren un rol estratégico de acuerdo a la importancia de algún tópico, ya sea por el interés que le otorga cierta administración de gobierno, o porque tienen carácter de institución permanente de acuerdo al ordenamiento legal.

Las instituciones consideradas clave se asocian a las encargadas de mantener la estabilidad en el país, siendo éstas, las de seguridad, defensa, inteligencia y economía. Por lo tanto, si se desea preservar la seguridad en el ámbito cibernético, se requiere de instituciones con una gran respuesta operativa ante las acciones ilícitas en el ciberespacio.

Ante dicho escenario, México tiene diversas instancias que abordan el tema de la ciberseguridad desde distintos enfoques. Algunas desarrollan el tópico desde una perspectiva de la seguridad pública, el cual tiene por objetivo evitar el hurto de información, la protección de las redes e *Internet*, así como llevar a cabo investigaciones que permitan entender la dinámica de los delitos en el ciberespacio.

Por otra parte, existen instituciones que basan el desarrollo de la ciberseguridad desde el ámbito de la defensa y la seguridad del Estado mexicano. Ante dicha dinámica, la Secretaría de Marina, la Secretaría de la Defensa Nacional, el Centro de Investigaciones y Seguridad Nacional, la Policía Federal y la Universidad Nacional Autónoma de México son las que tienen una función estratégica en dicha materia para efectos de esta investigación.

De acuerdo a sus ordenamientos legales, cada entidad tiene funciones específicas que les permiten abordar el ciberespacio con base a sus atribuciones. Cabe destacar que la cooperación e intercambio de información son el elemento esencial para construir líneas de acción, así como desarrollar capacidades de manera conjunta.

4.2.1 Policía Federal

Su función se encuentra establecida en la Ley de la Policía Federal y el artículo 2, específica lo siguiente:

> La Policía Federal es un órgano administrativo desconcentrado de la Secretaría de Seguridad Pública, y sus objetivos serán los siguientes: I. Salvaguardar la vida, la integridad, la seguridad y los derechos de las personas, así como preservar las libertades, el orden y la paz públicos; II. Aplicar y operar la política de seguridad pública en materia de prevención y combate de delitos; III. Prevenir la comisión de los delitos, y; IV. Investigar la comisión de delitos bajo la conducción y mando del Ministerio Público de la Federación, en términos de las disposiciones aplicables.[248]

En el artículo 8 (compuesto por 47 fracciones), se describen sus atribuciones y obligaciones; para efectos de esta investigación, se señalan las fracciones I, II, III, IV, V, VI, VII, VIII, que se refieren a la investigación, análisis y generación de inteligencia estratégica para prevenir y resolver delitos, y la XLII, que habla de la vigilancia, monitoreo y rastreo de la Red Pública y el *Internet* sobre sitios web en el que se identifiquen posibles actividades delictivas.[249]

Para atender las obligaciones de la fracción XLII, la Policía Federal cuenta con el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX), el cual se encarga de vigilar y salvaguardar la integridad de la infraestructura tecnológica del país.[250]

Forma parte de la comunidad del Foro de Respuesta a Incidentes y Equipos de Seguridad (FIRST, por sus siglas en inglés), permitiéndole interactuar con otros miembros para fortalecer la cooperación en materia técnica, operativa y de información con los demás centros o policías cibernéticas de otros países. En este sentido, también tiene su acreditación ante la Secretaría de Seguridad Multidimensional en la Organización de los Estados Americanos.

Otro de los objetivos del CERT-MX consiste en impulsar acciones conjuntas con el sector privado para generar conciencia sobre los potenciales peligros que puedan surgir, por ello, se procura desarrollar una cultura de prevención del delito cibernético que tenga impacto en los sectores productivos del país.[251] Si se trabaja y coordina no sólo con el sector privado dicho objetivo, es posible expandir los conocimientos sobre los riesgos existentes en el ciberespacio, de modo que la sociedad civil, las empresas y otras instituciones públicas tengan los conocimientos necesarios para evitar ser víctimas de ataques cibernéticos.

---

[248] "Ley de la Policía Federal", *Cámara de Diputados del H. Congreso de la Unión*, p. 1, http://bit.ly/2ktGdNU
[249] Ibíd., p. 3.
[250] "Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal", *Policía Federal*, 17 de mayo de 2018, acceso el 02 de octubre de 2018 en: http://bit.ly/2kecNDh
[251] Ibíd.

Otra base que da firmeza a las acciones del CERT-MX es contar con la certificación ISO/IEC 27001:2013, que emite la *British Standards Institution* en seguridad de la información.[252] De tal manera que, pone a la vanguardia sus normas de acuerdo a los estándares de la Organización Internacional de Normalización (ISO, por sus siglas en inglés).[253]

La especialización del CERT-MX en los diferentes rubros que aborda, han hecho posible trabajar, a nivel federal, en el asunto de la ciberseguridad. En el año 2016, la Policía Federal logró detener a 5 presuntos sujetos que formaban parte de una red internacional de ciberdelincuentes que llevaban acciones ilícitas de fraude cibernético.[254]

El CERT-MX tiene áreas especializadas en temas de prevención e investigación para las acciones ilícitas que se lleven a cabo en el ciberespacio; aunado a esto, tiene la autoridad a nivel federal para realizar labores de intercambio de información con policías cibernéticas nacionales, con organismos y entidades homologas internacionales en ese rubro.[255] Es por ello que su rol es vital en el tema de la ciberseguridad, puesto que puede desempeñar acciones de cooperación con otros centros cibernéticos a nivel internacional.

En tal sentido, las acciones de Policía Federal adquieren un valor significativo no sólo por la prevención del delito, sino porque también es la institución que debe asegurarse de monitorear las acciones que se desarrollan en el ciberespacio a través del CERT-MX a fin de evitar que se materialicen actividades ilícitas como pornografía infantil, fraude, falsificación, ataques cibernéticos en contra de infraestructuras críticas y la población.

Por ello, es necesario destacar la relevancia de su División Científica, la cual mediante la aplicación de metodologías científicas y tecnológicas permite establecer mejores resultados en cuanto a la prevención e investigación del delito cibernético.[256] En ese tenor, también es importante salvaguardar la información, por lo que su intervención en dicho tema hace

[252] Trujillo, "El ciberespacio, recurso y responsabilidad…", p. 5.
[253] «La ISO/IEC 27001:2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO / IEC 27001: 2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza». En "ISO / IEC 27001: 2013", *Organización Internacional de Normalización*, s.f., acceso el 02 de octubre de 2018 en: http://bit.ly/2kFJ9qx
[254] Trujillo, "El ciberespacio, recurso y responsabilidad…", p. 5.
[255] Ibíd.
[256] "División Científica", *Policía Federal*, s.f., acceso el 02 de septiembre de 2019 en http://bit.ly/2ktHswA

posible promover mejoras continuas en el tema del ciberespacio, especialmente en materia de ciberseguridad.

Por lo tanto, ante un mundo globalizado donde las amenazas son múltiples, el riesgo de padecer ataques cibernéticos es generalizado debido a que todos pueden ser víctimas, tal como lo demostró el virus *WannaCry*. Dicho escenario hace obligatorio que la Policía Federal siga en constante actualización, toda vez que es el primer escudo que tiene México en materia cibernética. Ante ello, su rol estratégico consiste en: prevención (monitoreo continuo del ciberespacio; campañas de concientización hacia la población por riesgos en el ciberentorno), investigación (cooperación interinstitucional e internacional) y respuesta.

4.2.2 CISEN

El Centro de Investigación y Seguridad Nacional (CISEN), es un órgano de inteligencia civil que está al servicio del Estado mexicano para preservar la integridad y estabilidad del país a través de la elaboración de inteligencia estratégica, táctica y operativa que sean determinantes para fortalecer el Estado de Derecho, y con ello, asegurar la gobernabilidad.[257]

Su principal función consiste en proponer medidas de prevención, disuasión, contención y neutralización de riesgos y amenazas que tengan como propósito incidir en el orden constitucional o causar problemas en el territorio y soberanía nacional, de modo que se busca evitar que el desarrollo económico, social y político del país, sea vulnerado.[258]

En la Ley de Seguridad Nacional, elaborada en el año 2005, se enuncian las atribuciones del CISEN. En el artículo 19, fracción III, se fija el valor del análisis prospectivo para la definición de posibles riesgos a la seguridad nacional. A saber:

> Preparar estudios de carácter político, económico, social y demás que se relacionen con sus atribuciones, así como aquellos que sean necesarios para alertar sobre los riesgos y amenazas a la Seguridad Nacional.[259]

Posteriormente, la fracción VII estipula:

[257] "¿Qué es el CISEN?", *Centro de Investigación y Seguridad Nacional*, s.f., acceso el 02 de octubre de 2018 en: http://bit.ly/2lPMbsr
[258] Ibíd.
[259] "Ley de Seguridad Nacional", *Cámara de Diputados del H. Congreso de la Unión*, p. 7, http://bit.ly/2kaR7I1

> Proponer al Consejo el establecimiento de sistemas de cooperación internacional, con el objeto de identificar posibles riesgos y amenazas a la soberanía y seguridad nacionales.

Ambas fracciones enfatizan dos criterios claves, la realización de estudios para definir riesgos que atenten contra la seguridad nacional, y la cooperación internacional como mecanismo de asistencia para la elaboración de rigurosos análisis que consideren el escenario internacional.

Por otra parte, las siguientes dos fracciones del artículo 19, hacen referencia a las tecnologías y comunicaciones como puntos vitales para la protección de la información:

> VIII. Adquirir, administrar y desarrollar tecnología especializada para la investigación y difusión confiable de las comunicaciones del Gobierno Federal en materia de Seguridad Nacional, así como para la protección de esas comunicaciones y de la información que posea;
> IX. Operar la tecnología de comunicaciones especializadas, en cumplimiento de las atribuciones que tiene encomendadas o en apoyo de las instancias de gobierno que le solicite el Consejo.[260]

Al considerar el carácter prospectivo y de generación de inteligencia estratégica, el CISEN realiza aportes mediante estudios que desarrolla del entorno nacional e internacional para la elaboración de la Agenda Nacional de Riesgos (ANR).

La ANR es aprobada de manera anual por el Titular del Ejecutivo Federal a propuesta del Secretario Técnico, en el marco del Consejo de Seguridad Nacional (CSN). Dicho Consejo está conformado por el Presidente de la República; el Secretario de Gobernación; el Secretario de la Defensa Nacional; el Secretario de Marina; el Secretario de Seguridad Pública; el Secretario de Hacienda y Crédito Público; el Secretario de la Función Pública; el Secretario de Relaciones Exteriores; el Secretario de Comunicaciones y Transportes; el Procurador General de la República y finalmente, el Director General del Centro de Investigación y Seguridad Nacional.[261]

El CISEN define como amenazas a la seguridad nacional: «Fenómenos intencionales generados por el poder de otro Estado, o por agentes no estatales, cuya voluntad hostil y

[260] Ibíd.
[261] Ibíd.

deliberada pone en peligro los intereses permanentes tutelados por la Seguridad Nacional, en parte o en todo el país, y cuestionan la existencia del mismo Estado.[262]

Dicho fundamento destaca que las ofensivas de otro Estado o agente no estatal que, tengan como objetivo entorpecer la estabilidad del país, perjudican y evitan que el interés nacional sea promovido, y con ello, puede poner en riesgo la integridad del Estado mexicano. En la variante cibernética, el uso de ciberpoder para ejercer coerción también debe ser considerado una amenaza debido a los impactos negativos que se pueden desarrollar en el ciberespacio.

Los riesgos a la seguridad nacional son denominados por este centro de inteligencia como:

> […] una condición interna o externa generada por situaciones políticas, económicas, sociales o agentes no estatales, así como por desastres naturales, de origen humano o epidemias, que sin tener carácter de amenazas pudieran poner en entredicho el desarrollo nacional.[263]

Los aportes de la ANR y la conformación del CSN, son base esencial para determinar cuáles son los riesgos que pueden perjudicar el desarrollo del país y representar un problema directo en la integridad y soberanía del Estado. Por lo tanto, el rol del CISEN tiene su fundamento en la seguridad nacional, con el desarrollo de inteligencia estratégica como coadyuvante prospectivo en la formulación de análisis que atiendan las necesidades de la coyuntura nacional e internacional para la reducción de riesgos y atenuación de amenazas, además de cuidar y fortalecer las comunicaciones del Gobierno Federal.

4.2.3 SEDENA

Las funciones y atribuciones de la Secretaría de la Defensa Nacional (SEDENA), están redactadas en la Ley Orgánica del Ejército y Fuerza Aérea Mexicanos. El artículo 1 específica el carácter permanente de las instituciones armadas y sus propósitos generales, siendo los siguientes:

> I. Defender la integridad, la independencia y la soberanía de la nación; II. Garantizar la seguridad interior; III. Auxiliar a la población civil en casos de necesidades públicas; IV. Realizar acciones cívicas y obras sociales que tiendan al progreso del país; y V. En caso de desastre, prestar ayuda para el

[262] "Amenazas y Riesgos", *Centro de Investigación y Seguridad Nacional,* s.f., acceso el 02 de octubre de 2018 en: http://bit.ly/2lPMdAz
[263] Ibíd.

> mantenimiento del orden, auxilio de las personas y sus bienes y la reconstrucción de las zonas afectadas.[264]

Así mismo, en el capítulo IV, artículo 95 Bis, se mencionan las acciones a desarrollar en el ámbito informático, a saber:

> I. Diseñar, desarrollar, recibir, almacenar, abastecer, evacuar, reparar, recuperar y controlar los bienes y servicios informáticos del Ejército y Fuerza Aérea; II. Fijar normas técnicas para los bienes y servicios informáticos; III. Planear, organizar, implementar, conservar, explotar y adaptar bienes y servicios informáticos del Ejército y Fuerza Aérea, así como los que queden bajo control militar; IV. Auxiliar en los procedimientos de auditoría y seguridad informática; V. Auxiliar a los mandos en todos los niveles en el empleo, operación y conservación de los bienes informáticos, capacitar al personal del servicio y fomentar la cultura informática, y VI. Las demás que le confieran esta Ley y cualquier disposición aplicable.

El trabajo informático que desarrollan es para la misma Secretaría, es decir, toda aquella infraestructura, red o dispositivo que sea utilizado por la SEDENA debe ser protegido para salvaguardar el flujo de información que se genera. Esto a través de la gestión, mantenimiento y capacitación del personal, con el fin de establecer una cultura informática en la institución.

Las labores generales se encuentran establecidas en la ley, no obstante, en la cuestión operativa, la hoja de ruta a seguir se desprende del Plan Nacional de Desarrollo (PND) que el Gobierno de la República haya presentado de acuerdo al plan sexenal. En este caso, el PND 2013-2018, corresponde al del gobierno del ex presidente Enrique Peña Nieto.

Derivado del PND, se desarrolla el Programa Sectorial de Defensa Nacional 2013-2018, el cual, en el primer capítulo «Diagnóstico», en la sección «Inteligencia y Ciberespacio», se menciona:

> […] la seguridad en el ciberespacio en México no se ha abordado desde el punto de vista de la defensa nacional, ya que sólo se ha atendido desde el ámbito de la seguridad institucional y persecución del delito, no obstante que en la agenda nacional de riesgos 2012, se planteó que la vulnerabilidad cibernética puede impactar en la defensa del Estado Mexicano.[265]

[264] "Ley Orgánica del Ejército y Fuerza Aérea Mexicanos", *Cámara de Diputados de H. Congreso de la Unión*, p. 1 http://bit.ly/2kedpJ5

[265] "Programa Sectorial de Defensa Nacional 2013-2018", *Secretaría de la Defensa Nacional*, 2013, p. 21, http://bit.ly/2lHfLR9

El programa también precisa que la secretaría cuenta con dos Direcciones Generales encargadas de administrar las Tecnologías de la Información y la Comunicación; sin embargo, no cuenta con un organismo que atienda las actividades de seguridad y defensa en el ciberespacio.[266]

Para afrontar el problema de no contar con un organismo especializado en el ciberentorno, el capítulo tercero «Objetivos, Estrategias y Líneas de Acción», desarrolla una serie de puntos a considerar.

El objetivo 1, precisa, «contribuir a preservar la integridad, estabilidad, independencia y soberanía del Estado Mexicano». De esta manera, en la estrategia 1.6, que tiene como línea de acción 1.6.5., establece, «impulsar el marco legal para el desarrollo de la cuarta dimensión de operaciones denominada 'ciberespacio'».[267]

En su objetivo 2, menciona que «el desarrollo de la Cuarta Dimensión de Operaciones Militares 'Ciberespacio' parte del interés de contribuir en la protección de los activos informáticos y de comunicaciones de ataques que pretendan vulnerar los centros de control estratégico». Aunado a esto, la estrategia 2.1., en su línea de acción 2.1.7., estipula que se debe fortalecer la Escuela Militar de Inteligencia a través de la capacitación y adiestramiento del personal en asuntos de inteligencia, contrainteligencia y ciberespacio; además, la línea de acción 2.1.10., señala que se debe impulsar el desarrollo de la Cuarta Dimensión de Operaciones con recursos humanos y tecnológicos.[268]

Para llevar a cabo dichos objetivos y líneas de acción, se requieren recursos y presupuesto. Por lo tanto, en el año 2017, la SEDENA solicitó 533.2 millones de pesos para desarrollar sus metas en el ámbito del ciberespacio, sin embargo, no se les asignó ningún recurso en ese rubro.[269]

La falta de asignación de presupuesto para el desarrollo del ciberespacio merma la oportunidad de que la Secretaría de la Defensa Nacional construya las capacidades suficientes para hacer frente a ciberataques que tengan por objetivo la infraestructura crítica

[266] Ibíd.
[267] Ibíd., p. 33.
[268] Ibíd., p. 35.
[269] Julio Sánchez, "Política de ciberseguridad en México tiene un camino sinuoso", *El Economista*, 27 de diciembre de 2016, http://bit.ly/2kfuSkm

de las Fuerzas Armadas. Para ejemplificar esto, de acuerdo al «Informe de Avance y Resultados 2018» de dicha secretaría, señala que sólo se logró avanzar un tres por ciento en la capacitación de personal del Centro de Operaciones del Ciberespacio. Por otra parte se precisa que sólo se pudo avanzar un setenta y cinco por ciento en el desarrollo de la cuarta dimensión de operaciones militares, toda vez que fue insuficiente el presupuesto para cumplir la meta del cien por ciento.[270] También se argumenta que hubo un avance del setenta por ciento en un proyecto que se denomina «adquisición de equipo de seguridad informática».[271]

Esto demuestra que los trabajos planteados por la SEDENA no se cumplieron de manera total debido a que no se asignó el presupuesto suficiente para desarrollar de manera eficiente lo relativo a ciberseguridad y ciberdefensa. Si bien hubo un avance en la administración del ex presidente Enrique Peña Nieto, faltó realizar inversión en materiales informáticos para prueba, desarrollo y gestión de operaciones y simulaciones cibernéticas, así como para capacitar a personal de la institución, puesto que tienen un rol estratégico y permanente en la defensa nacional.

Los trabajos desarrollados[272] por la SEDENA muestran que la institución se encuentra en una fase de aprendizaje en el tópico de la cuarta dimensión de operaciones. En ese tenor, es necesario destinar más recursos para que se pueda desarrollar la fórmula de inversión, desarrollo e innovación en materia del ciberespacio; en tal sentido dicha secretaría se encuentra en una pre fase de la fórmula antes mencionada, puesto que está adquiriendo los conocimientos necesarios para entender el ciberentorno desde la perspectiva militar, posteriormente, si se realiza la inversión necesaria, es posible que la SEDENA logre pasar a un modelo que desarrolle capacidades con base a los conocimientos adquiridos.

4.2.4 SEMAR

Las atribuciones de la Secretaría de Marina (SEMAR) se encuentran establecidas en la Ley Orgánica de la Armada de México. De manera similar a la SEDENA, su carácter es de

[270] "Informe de Avance y Resultados 2018", *Secretaría de la Defensa Nacional*, 2018, p. 9, acceso el 03 de septiembre de 2019, http://bit.ly/2lG9UeJ
[271] Ibíd.
[272] En el Capítulo 5 de esta investigación, en la sección de informes de gobierno, se citan las labores más importantes de la Secretaría de la Defensa Nacional en materia de ciberseguridad.

institución permanente y su propósito principal es usar el poder naval de la Federación para la defensa exterior, y como soporte para la seguridad interior del país.

En el artículo 2 de la ley, se tipifican dieciséis atribuciones; sin embargo, se destacan las siguientes en el ámbito de la seguridad:

> I. Organizar, adiestrar, alistar, equipar y operar a las fuerzas que la constituyen para el cumplimiento de su misión y ejercicio de sus funciones; II. Cooperar en el mantenimiento del orden constitucional del Estado Mexicano; III. Realizar acciones para salvaguardar la soberanía y defender la integridad del territorio nacional en el mar territorial, zona marítimo-terrestre, islas, cayos, arrecifes, zócalos y plataforma continental; así como en aguas interiores, lacustres y ríos en sus partes navegables, incluyendo los espacios aéreos correspondientes, así como vigilar los derechos de soberanía en la zona económica exclusiva; VI. Proteger instalaciones estratégicas del país en su ámbito de competencia y donde el Mando Supremo lo ordene.[273]

De esta manera, en el Programa Sectorial de Marina 2013-2018, se formulan los criterios a desarrollar en el ámbito del ciberespacio. En el segundo capítulo, «Fortalecer las capacidades de respuesta operativa institucional, contribuyendo a garantizar la Seguridad Nacional y la protección al medio ambiente marino», se tipifica en el objetivo 2, la necesidad de fortalecer las capacidades de respuesta operativa institucional en materia de Seguridad Nacional.

De modo que en la estrategia 2.6., en su línea de acción 2.6.5., establece, «Impulsar la creación de la normatividad que respalde la estrategia de Inteligencia Naval en materia de Ciberseguridad y Ciberdefensa».[274] Los demás objetivos, estrategias y líneas de acción pueden visualizarse en el siguiente cuadro.

CUADRO 10. OBJETIVOS, ESTRATEGIAS Y LÍNEAS DE ACCIÓN DEL PROGRAMA SECTORIAL DE MARINA 2013-2018.[275]

Objetivo 3. Consolidar la Inteligencia Naval para identificar, prevenir y contrarrestar riesgos y amenazas que afecten a la Seguridad Nacional.	Estrategia 3.4. Consolidar el Sistema Integral de Seguridad de la Información Institucional que fortalezca la Estrategia Nacional de Seguridad de la Información	Líneas de Acción: 3.4.1. Modernizar con equipamiento, capacitación y tecnologías del Sistema Integral de Seguridad de la Información Institucional, acorde a la estrategia nacional;

[273] "Ley Orgánica de la Armada de México", *Cámara de Diputados del H. Congreso de la Unión*, p. 1, http://bit.ly/2lHAyEa
[274] "Programa Sectorial de Marina 2013-2018", *Secretaría de Marina*, p. 44, http://bit.ly/2kakdqX
[275] Ibíd.

		3.4.2. Fortalecer el Sistema Integral de Seguridad de la Información y la seguridad de las infraestructuras críticas de información institucional; 3.4.3. Fortalecer la coordinación interinstitucional e internacional para impulsar la Estrategia de Seguridad de la Información.
	Estrategia 3.5. Emplear e incrementar las capacidades de Ciberseguridad y Ciberdefensa, contribuyendo a la seguridad del ciberespacio del Estado Mexicano.	Líneas de acción: 3.5.1. Construir un Centro de Control de Ciberdefensa y Ciberseguridad para fortalecer la cuarta dimensión de operaciones de ciberseguridad; 3.5.2. Adquirir infraestructura tecnológica y capacitación para implementar acciones de seguridad en el ciberespacio; 3.5.3. Implementar una estrategia de Ciberdefensa y Ciberserguridad que impulse la normatividad de acuerdo a sus atribuciones.

De manera similar a la SEDENA, la SEMAR solicitó 9.1 millones de pesos para equipamiento en el desarrollo de ciberinteligencia; sin embargo, los recursos no fueron asignados.[276]

Respecto al «Informe de Avance y Resultados 2018», se destaca en materia de ciberespacio que la mayor parte de las metas se logró, de acuerdo a la sección Seguridad de la información y del ciberespacio, la SEMAR señala que se cumplió en un 103.68 el objetivo.[277] A diferencia del informe sectorial de la SEDENA, la Secretaría de Marina no señala de manera precisa los avances en materia de ciberseguridad y ciberdefensa, de manera general sólo muestra que el resultado se alcanzó.

Por otra parte, enfatiza la participación de personal naval en ejercicios, conferencias y cursos en dicha materia. Para efectos de esta investigación y teniendo en cuenta la relación bilateral con Estados Unidos es importante señalar tres reuniones que se llevaron a cabo por el

[276] Sánchez, "Política de ciberseguridad en México…".
[277] "Informe de Avance y Resultados 2018", *Secretaría de Marina*, 2018, p. 23, acceso el 03 de septiembre de 2019, http://bit.ly/2lNL3pe

acuerdo de colaboración Secretaría de Marina-Comando Norte de los Estados Unidos (SEMAR-*USNORTHCOM*, por sus siglas en inglés), las cuales son: el ejercicio *TRADEWINDS* 2018 y los cursos *Cyber Network* y *Cyber Security*.[278]

El párrafo anterior ejemplifica la estrecha relación entre la SEMAR y el Comando Norte de los Estados Unidos. En ese sentido, se muestra que la Secretaría de Marina es dinámica en cuanto a las reuniones con dicho Comando, por lo que puede resultar benéfico en el corto y mediano plazo debido a que se pueden adoptar nuevas estrategias en materia de la cuarta dimensión de operaciones derivado del aprendizaje obtenido por los ejercicios e intercambio de conocimientos.

En el marco de la relación bilateral es evidente que el referente para México es Estados Unidos, no obstante también se puede dinamizar y diversificar el conocimiento si se tienen en cuenta a países como Francia, Canadá, Israel, Alemania, entre otros. El punto medular consiste en que al igual que la SEDENA, es importante aplicar la fórmula de inversión, desarrollo e innovación para fortalecer el ciberespacio desde el ámbito naval. Teniendo en cuenta ambas instituciones, la cooperación interinstitucional generaría un mayor soporte en cuanto a la creación de capacidades en conjunto para el desarrollo futuro de ejercicios y operaciones entre secretarías.

4.2.5 UNAM

La Universidad Nacional Autónoma de México (UNAM), es una institución académica que da servicio a una gran cantidad de alumnos de nivel medio y superior, de modo que tiene grandes flujos de información en sus servidores y plataformas *web*. Asimismo, pone a disposición del público general, investigaciones, publicaciones y otros materiales que se registran en la base de datos de sus sistemas informáticos.

Esto requiere de altos niveles de seguridad cibernética para mantener y salvaguardar la información con el propósito de evitar que los datos sean expuestos o vulnerados en sus sistemas y ordenadores. Las labores en ese rubro son atendidas por la Coordinación de Seguridad de la Información (CSI), la cual, forma parte de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación.

[278] Ibíd.

A su vez, la UNAM es miembro del Foro de Respuesta a Incidentes y Equipos de Seguridad (FIRST), lo que supone un gran logro porque permite la interacción con otras instituciones que conforman dicha comunidad. En ese sentido, también tienen su registro ante la Secretaría de Seguridad Multidimensional de la OEA; esto pone de manifiesto la importancia de la institución en materia de ciberseguridad. Aunado a ello, cuenta con otras certificaciones en seguridad de la información (ISO 27001), respaldada por la Asociación Española de Normalización y Certificación (AENOR) con sede en México, así como de la Red Internacional de Certificación (IQNET, por sus siglas en inglés).[279]

Su rol como institución académica no sólo se basa en proveer seguridad en sus sistemas, también impulsa la difusión de la cultura de seguridad en los sistemas de cómputo a través de los servicios que ofrece en forma de seminarios, cursos, investigaciones, desarrollo de proyectos, entre otros.

Las actividades que realiza en el ámbito de la seguridad informática, están basadas en los siguientes objetivos:

> Proporcionar servicios de seguridad de la información para la UNAM y otras organizaciones; promover la cultura de seguridad de la información; formar especialistas que desarrollen y apliquen estrategias de protección de la información; difundir contenidos especializados en seguridad de la información; colaborar con instituciones nacionales e internacionales en materia de detección y respuesta a incidentes, y; elaborar políticas y lineamientos de seguridad de la información para las dependencias y entidades académicas universitarias.[280]

Con base a lo anterior, su sitio *web* tiene diversos servicios que están al alcance de todos, pues pone a disposición general boletines informativos, terminología explicada mediante su diccionario electrónico, información sobre seguridad cibernética en las revistas que publica, y la disponibilidad para reportar incidentes informáticos en la RedUNAM e *Internet* a través de su correo institucional.

Identificar las instituciones estratégicas en materia de ciberseguridad en México, permite entender el compromiso del Estado para hacer frente a los riesgos provenientes del ciberespacio. En ese tenor, cada una tiene un objeto y metodología para atender el asunto.

---

[279] "Coordinación de Seguridad de la Información UNAM-CERT"*, Universidad Nacional Autónoma de México*, s.f., acceso el 04 de octubre de 2018 en: http://bit.ly/2kDfo9X

[280] Ibíd.

Las primeras cuatro instituciones corresponden al mantenimiento de la seguridad pública y nacional desde el enfoque de la seguridad y la defensa; mientras que la UNAM, asume una posición formativa y educacional en materia de seguridad cibernética.

Dichas instituciones abordan el tema desde un objetivo definido, por lo que su alcance se encuentra ya establecido, de modo que no aborda de manera especializada la esfera económica. Para esto, es necesario identificar quién se encarga del sistema financiero, así como definir cuáles son las infraestructuras críticas del Estado mexicano.

4.3 Infraestructura crítica y sistema financiero

La infraestructura crítica (IC) es necesaria para el correcto funcionamiento de los sistemas productivos y de servicios de un país, por lo que si no son efectivos o son vulnerados, éstos pueden afectar el desarrollo del Estado.

Dicho lo anterior, es preciso definir qué es una infraestructura crítica. En tal sentido, Aguirre menciona lo siguiente:

> […] es el conjunto de activos tecnológicos indispensables, que interactúan entre sí para brindar servicios vitales a los habitantes de un país. Los activos pueden ser instalaciones físicas o virtuales, redes de datos, redes industriales, sistemas de información, bases de datos, sistemas de control industrial, procesos automatizados o cualquier otro componente tecnológico que permite la prestación o el monitorio de un servicio esencial para el bienestar de la población y el sostenimiento de la economía de un país.[281]

Aunado a la definición anterior, el Centro de Ciberseguridad Industrial estipula que el término de Infraestructura Crítica es utilizado por los Estados para delimitar las instalaciones o sistemas que prestan servicios esenciales, por lo que si son afectados, se vuelve difícil implementar una solución alterna.[282]

Las IC parten del supuesto de funcionalidad debido a que en la era digital, la mayor parte de los procesos se están diseñando para que sean utilizados mediante el empleo de sistemas de interconexión entre ordenadores y *software*. Esto ha permitido que los servicios de

[281] Aguirre, "Ciberseguridad en Infraestructuras…", p. 7.
[282] "La Protección de Infraestructura Críticas y la Ciberseguridad Industrial", *Centro de Ciberseguridad Industrial*, 2013, p. 8, http://bit.ly/2mbiF0E

telecomunicaciones, de salud, financieros, de energéticos, industriales y de seguridad, se desarrollen con códigos y algoritmos computacionales que permitan un rendimiento óptimo.

Las IC se pueden clasificar de dos maneras, de servicio y de información. Respecto a las primeras, su aspecto operativo resulta indispensable para los sectores productivos y la ciudadanía debido a que si se altera su correcto funcionamiento, podría ocasionar situaciones negativas de alto impacto; las segundas, hacen referencia al flujo de datos que navegan por los ordenadores y las redes públicas o privadas, de las cuales, el riesgo puede ser variado dependiendo del tipo de información que se encuentre en los dispositivos, pues podría ser de carácter sensible o restringido.[283]

En tal sentido y considerando las dos clasificaciones, las IC son indispensables para los Estados, puesto que la mayor parte de ellas, se emplea para proveer distintos servicios a la población, además de los datos que se comparten entre instituciones de alto nivel, que requieren de la difusión rápida de la información para la toma de decisiones. Por lo tanto, para dilucidar la importancia de las infraestructuras críticas, es necesario señalar cuáles son los sectores más esenciales. El primero de ellos tiene que ver con las telecomunicaciones; el segundo con la energía; el tercero abarca los servicios financieros; el cuarto, el transporte; el quinto, los sistemas de aguas; el sexto, el ámbito de la seguridad y la defensa; y el séptimo con la industria[284], el cual adquiere relevancia por el sentido de la productividad.[285]

Si consideramos que tales sectores, de manera gradual, comienzan a innovar sus sistemas informáticos y tecnológicos, entonces se vuelve un requisito obligatorio invertir también en mejores esquemas y protocolos de seguridad; en este caso, es necesario fortalecer los planes de acción y gestión de riesgos en ciberseguridad para evitar ataques cibernéticos. Las IC pueden tener como base sistemas digitales, los cuales pueden ser vulnerados por la aplicación de códigos altamente especializados, o en el peor de los casos si se encuentran los denominados *Zero-days*, de modo que pueden ser manipulados para que obedezcan las instrucciones de su irruptor. En ese sentido, si los sistemas con los que operan dichas infraestructuras son corrompidos, entonces pueden alterar su correcto funcionamiento, por

[283] Aguirre, "Ciberseguridad en Infraestructuras…", p. 8.
[284] Ibíd.
[285] Es necesario precisar que, la manera en que se enlistan los sectores no representa un orden de importancia, sino que sólo se enumeran para destacar algunos, debido a que pueden existir otros. Dependerá de cada Estado determinar cuáles adquieren mayor relevancia de acuerdo a sus intereses y necesidades.

lo que es posible que sus servicios no sean óptimos y como consecuencia de ello, pueden entorpecer las actividades de un Estado, en particular, las más esenciales.

Los casos de Estonia, *Stuxnet* y *WannaCry* son ejemplos formidables de vulneración en servicios e información, cada uno con su particularidad, generaron situaciones críticas en el ámbito político, social y económico. *WannaCry* tuvo incidencia en IC de información y servicios, pues cifró los archivos y no permitió abrirlos, ocasionado daños directos en las actividades productivas, como el caso de la empresa Renault en Francia.

Las amenazas a las IC se pueden materializar a través del uso de espionaje industrial, sabotaje de las redes y sistemas computacionales, robo de datos, utilización de códigos maliciosos, indisponibilidad de servicio[286] y destrucción de los sistemas físicos que utilizan sistemas informáticos, tal como sucedió con las centrifugadoras de Irán.

El Programa para la Seguridad Nacional 2014-2018, en su análisis específica que el país tiene aproximadamente tres mil instalaciones estratégicas. Petróleos Mexicanos (PEMEX) cuenta con un cuarenta y siete por ciento; la Comisión Nacional del Agua (CONAGUA) tiene un diecisiete por ciento, y la Comisión Federal de Electricidad un trece por ciento.[287] Del porcentaje restante no se menciona qué instituciones albergan las demás instalaciones clave.

Finalmente, lo más reciente para las IC en México se sitúa en el año 2018, cuando el Servicio de Protección Federal (SPF), concluyó el «Taller Seguridad y Resiliencia de Infraestructuras Críticas», el cual, fue llevado a cabo por el Buró de Seguridad Diplomática de los Estados Unidos de América, a través del Programa Antiterrorismo (ATA, por sus siglas en inglés). De esta manera, se ha capacitado a personal del SPF desde el año 2015, con el propósito de que a largo plazo, los miembros del Servicio sean los que suministren conocimientos a integrantes y encargados de instalaciones estratégicas del Estado mexicano.[288]

Es necesario destacar que el desarrollo de la ciberseguridad implica identificar qué y cuáles son las IC vitales del país para que, con su detección, sea posible desarrollar mejores

[286] Ibíd., p. 13.
[287] "Programa para la Seguridad Nacional 2014-2018", *Presidencia de la* República, 2014, p. 60, http://bit.ly/2IK44ce
[288] "CNS fortalece capacidades del sistema de protección física para infraestructuras vitales", *Servicio de Protección Federal*, 08 de febrero de 2018, acceso el 04 de octubre de 2018 en: http://bit.ly/2lPNCXR

esquemas de prevención y gestión de riesgos, además de su fortalecimiento en el plano informático, así como de capital humano a través de capacitación y especialización en dicha materia.

El Sistema Financiero

En este capítulo se señalaron las instituciones estratégicas en el ámbito de la seguridad y defensa; sin embargo, no atienden de manera particular las condiciones financieras porque no están dentro de sus atribuciones de manera estricta. El Sistema Financiero (SF) tiene una importancia vital por ser el que regula las transacciones económicas que desarrollan diversos actores en México.

La implementación de sistemas digitales y el dinamismo financiero han forjado una dependencia hacia las transacciones electrónicas debido a que es más fácil llevarlas a cabo a través de un dispositivo, así como también es más sencillo almacenar los datos sensibles sobre los clientes, de modo que las cuestiones operativas y de información es donde los atacantes centran su atención.

Por otra parte, la estabilidad macroeconómica y el gran flujo de capital, vuelven al país un objetivo atractivo para los delincuentes, debido a eso, se han propagado y materializado diversas amenazas. En este sentido, *Control Risks* menciona que:

> El crecimiento del rango de objetivos fomenta la propagación de las amenazas cibernéticas, así como el deseo de los delincuentes establecidos de diversificar sus operaciones. La importancia geopolítica y económica de las regiones en desarrollo alrededor del mundo, es una de las causas de esta diversificación.[289]

México goza de un espacio geográfico estratégico y cuenta con diversos tratados de libre comercio, lo que permite que su economía sea dinámica en cuanto a producción y servicios. Es por esto que el SF mexicano adquiere una relevancia significante, pues gran parte del mismo ya cuenta con componentes cibernéticos establecidos. Por lo tanto, es evidente que se deban fortalecer los sistemas informáticos que emplean tecnología digital para la realización de transacciones financieras electrónicas.

[289] "Amenazas Cibernéticas al sector financiero mexicano", *Control Risks*, 2015, p. 5, http://bit.ly/2lK4a3A

Banxico estableció el Sistema de Pagos Electrónicos Interbancarios (SPEI) en el año 2004, para sustituir al Sistema de Pagos Electrónicos de Uso Ampliado (SPEUA). Este sistema permite las transacciones bancarias en tiempo real y es regulado por el Banco de México, de modo que se pueden imponer sanciones cuando se amerite.[290] De esta manera, se estableció un control rígido en seguridad e infraestructura de los sistemas para que exista una fluidez operacional en las transacciones interbancarias.

En el año 2013, el Banco de México creó la Gerencia de Seguridad de Tecnologías de la Información para asesorar, administrar y dirigir proyectos con base a su estrategia institucional en el ámbito informático. El criterio de su establecimiento consistió en tener personal especializado para detectar y hacer frente a los riesgos derivados de las vulnerabilidades en el sistema financiero, por lo que se implementaron herramientas de protección cibernética para robustecer la seguridad.[291]

El Banxico, al ser una institución estratégica en el sistema financiero nacional, adquiere la responsabilidad de proteger las operaciones que realicen los diversos actores que interactúan entre sí. Por lo tanto, en el año 2016, el Banco de México contrató a una consultora internacional para tener un diagnóstico general sobre la seguridad informática de la institución. El resultado generó certidumbre, puesto que los resultados mostraron que la institución tiene un nivel razonable de seguridad; sin embargo, la consultora precisó que es fundamental seguir mejorando, actualizando e innovando los sistemas, ya que, como entidad financiera, su rol es prioritario en el sistema financiero nacional.[292] En tal sentido, es oportuno mencionar que la variable de la innovación tecnológica financiera, hace obligatorio mejorar continuamente los niveles de seguridad cibernética para brindar confianza y certidumbre al sistema financiero mexicano.

Es por ello que en el año 2017, Banxico reforzó su estrategia de ciberseguridad, planteando como pilares fundamentales, los siguientes objetivos:

- Proteger la información y sus procesos; la ciberseguridad en el Banco de México protegerá las aplicaciones informáticas, así como la seguridad de la información.

[290] "¿Qué es el SPEI?", *El Economista*, 03 de mayo de 2018, acceso el 05 de octubre de 2018 en: http://bit.ly/2kDfiyY
[291] "Estrategia de Ciberseguridad del Banco de México", *Banco de México*, 2018, p. 2, http://bit.ly/2ktwerX
[292] Ibíd., p. 3.

- Tener una respuesta proactiva en la recolección de indicadores de compromiso o prevención de riesgos.
- Focalizar la seguridad de la información a todo el ecosistema para solicitar requerimientos de seguridad a las instituciones financieras que interactúan con Banxico.
- Reforzar la gobernabilidad de la seguridad de la información para el diseño de políticas institucionales de ciberseguridad a través de una ampliación de recursos humanos y reorganización de áreas. Con base en esto, se autorizó la creación de la Dirección de Ciberseguridad.[293]

Los ciberataques al SPEI permitieron que Banxico pudiera dimensionar los efectos negativos que un ataque cibernético puede ocasionar al sistema financiero. De tal manera que, dicho acontecimiento hizo posible que se creara la Dirección de Ciberseguridad. Ésta tiene como atribuciones, establecer políticas, lineamientos y estrategias para fortalecer la seguridad de la información que gestiona el banco central, además de ampliar la aplicabilidad de algunas medidas a las entidades intermediarias, siempre y cuando se encuentren dentro de las competencias del Banco de México.[294]

Por otra parte, en el año 2018, se aprobó la Ley Fintech[295] en el país. Se trata de una iniciativa para regular a las instituciones tecnológicas y financieras. En este sentido, se permitirá que se realicen diversos servicios financieros desde dispositivos móviles y también se podrán utilizar monedas virtuales como las *bitcoins*[296].

De acuerdo con *FinTech* de México, los elementos más importantes a considerar para el sector son los medios de pago y transferencias; la infraestructura para servicios financieros; la originación digital de créditos; las soluciones financieras para empresas; las finanzas

[293] Ibíd., p. 4.
[294] "Banxico crea oficina de ciberseguridad tras hackeo a bancos", *Forbes México*, 15 de mayo de 2018, acceso el 05 de octubre de 2018 en: http://bit.ly/2kFV33E
[295] El documento tiene 145 artículos y está compuesto por siete títulos. Su objetivo es regular la organización, funcionamiento y procesos operativos de las instituciones tecnológicas financieras. En "10 puntos para entender la nueva ley fintech", *El Financiero*, 01 de marzo de 2018, acceso el 05 de octubre de 2018 en: http://bit.ly/2kb7vbw
[296] «Bitcoin es una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios. Desde un punto de vista de usuario, Bitcoin es como dinero para Internet». En "¿Qué es bitcoin?", *bitcoin*, s.f., acceso el 05 de octubre de 2018 en: http://bit.ly/2lNjVqI

personales y asesoría; los mercados financieros, y las criptomonedas y *blockchain*.[297] Por lo tanto, el Banco de México y otras entidades financieras tendrán que trabajar en conjunto para regular las operaciones que lleven a cabo las empresas *fintech* en el país.

Otras instituciones que también están realizando acciones en materia de ciberseguridad son la Secretaría de Hacienda y Crédito Público (SHCP) y la Comisión Nacional Bancaria y de Valores (CNBV). Ambas, desarrollaron el foro «Fortaleciendo la ciberseguridad para la estabilidad del sistema financiero mexicano», con el propósito de compartir experiencias en dicha materia. Al respecto, se estipularon los siguientes cinco principios para fortalecer la ciberseguridad en el SF mexicano:

> Adoptar y mantener actualizadas políticas, métodos y controles para identificar, evaluar, prevenir y mitigar los riesgos de ciberseguridad, que se autoricen por los órganos de gobierno de mayor decisión y permeen a todos los niveles de la organización;
>
> Establecer mecanismos seguros para el intercambio de información entre los integrantes del sistema financiero y las autoridades, sobre ataques ocurridos en tiempo real y su modo de operación, estrategias de respuesta, nuevas amenazas, así como del resultado de investigaciones y estudios, que permitan a las entidades anticipar acciones para mitigar los riesgos de ciberataques; lo anterior, protegiendo la confidencialidad de la información;
>
> Impulsar iniciativas para actualizar los marcos regulatorios y legales que den soporte y hagan converger las acciones y esfuerzos de las partes, considerando las mejores prácticas y acuerdos internacionales;
>
> Colaborar en proyectos para fortalecer los controles de seguridad de los distintos componentes de las infraestructuras y plataformas operativas que soportan los servicios financieros del país, promoviendo el aprovechamiento de las tecnologías de información para prevenir, identificar, reaccionar, comunicar, tipificar y hacer un frente común ante las amenazas presentes y futuras, y;
>
> Fomentar la educación y cultura de ciberseguridad entre los usuarios finales, y el personal de las propias instituciones que, a través de una capacitación continua, redunde en una participación activa para mitigar los riesgos actuales de ciberataques.[298]

Por último, la CNBV estableció en el año 2018, la necesidad de que las entidades financieras cuenten con un oficial de seguridad de la información para fortalecer la seguridad cibernética. También se enlistaron tres tareas importantes que se deben cumplir: «implementar políticas y procedimientos de seguridad; crear un esquema de control de acceso a la infraestructura

[297] "¿Qué es Fintech?", *FinTech México,* s.f., acceso el 05 de octubre de 2018 en: http://bit.ly/2kb6KPP

[298] "Foro de Ciberseguridad", *Comisión Nacional Bancaria y de Valores,* 23 de octubre de 2017, acceso el 05 de octubre de 2018 en: http://bit.ly/2lHBqbU

tecnológica; y establecer los mecanismos para una identificación y validación de los incidentes de ciberseguridad». En tal sentido, un punto prioritario consiste en robustecer los mecanismos de inteligencia cibernética, con el fin de obtener una respuesta más rápida ante los incidentes financieros en el ciberespacio.[299]

[299] Fernando Gutiérrez, "CNBV: endurecer reglas en ciberseguridad del sistema financiero mexicano", *El Economista*, 22 de agosto de 2018, acceso el 05 de octubre de 2018 en: http://bit.ly/2m8DKst

CAPÍTULO 5

LA CIBERSEGURIDAD Y SUS DESAFÍOS A LA SEGURIDAD NACIONAL DE MÉXICO

La seguridad nacional es indispensable para el mantenimiento del orden y la paz de un Estado, por lo que es prioritario establecer estrategias, normas, políticas, inteligencia y metodologías para hacer frente a los escenarios adversos que se presenten a nivel interno y externo.

A principios del año 2000, con la transición democrática de la gobernanza del Partido Revolucionario Institucional (PRI) al Partido Acción Nacional (PAN), y con los sucesos del 11 de septiembre en los Estados Unidos, México tuvo que replantear su esquema tradicional de la seguridad, al incorporar nuevos riesgos y amenazas en los que figuran los actos de terrorismo.

La coyuntura innovadora de la Cuarta Revolución Industrial y el proceso de la globalización, han hecho que los fenómenos tradicionales de riesgos y amenazas tengan menos amplitud y discusión en los debates sobre seguridad; sin embargo, esto no quiere decir que no sigan representando un peligro potencial. Es por esto que la Seguridad Nacional de México debe estar a la vanguardia de los retos digitales, pues en toda guerra, un objetivo clásico consiste en atacar las comunicaciones existentes para generar crisis e incertidumbre al momento de tomar decisiones[300]; y es que actualmente, la mayor parte de las comunicaciones se encuentran en interconexión con el ciberespacio. Tal escenario hace obligatorio que la Seguridad Nacional de México deba prevenir toda eventualidad que pueda causar inestabilidad en la gobernabilidad del país.

5.1 Ley de Seguridad Nacional

La actual seguridad nacional de México está regida por la Ley de Seguridad Nacional del año 2005, y considera como amenazas las siguientes acciones, a saber:

> I. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional; II. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano; III. Actos que impidan a las autoridades actuar contra la delincuencia organizada; IV. Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la

[300] Óscar Sánchez Belmont, *Inteligencia y contrainteligencia*, Ediciones Gernika, México, 2014, p. 28.

> Constitución Política de los Estados Unidos Mexicanos; V. Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada; VI. Actos en contra de la seguridad de la aviación; VII. Actos que atenten en contra del personal diplomático; VIII. Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva; IX. Actos ilícitos en contra de la navegación marítima; X. Todo acto de financiamiento de acciones y organizaciones terroristas; XI. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia, y XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.[301]

A pesar de que se enlistan doce, no se hace mención sobre actos ilícitos en el ciberespacio. Esto es crítico debido a que el tiempo es una variable necesaria para el desarrollo de la seguridad, de modo que, al no considerarlo, se puede poner en riesgo la estabilidad del país. Por lo tanto, la Seguridad Nacional de México[302] tiene que estar al margen de los cambios globales, regionales y locales. También debe tomar en cuenta las innovaciones tecnológicas, pues es un factor que siempre tiende a modificarse.

En tal sentido, es preciso destacar que el concepto o la idea sobre la seguridad nacional es relativamente nuevo para México, puesto que la primera vez que se estableció fue en el Plan Global de Desarrollo del entonces presidente José López Portillo en la década de los años ochenta. Tal situación enfocaba dicho concepto en forma restringida, es decir, se le vinculaba únicamente con cuestiones de carácter militar, soberanía territorial y defensa externa,[303] lo cual es entendible teniendo en cuenta el contexto de la Guerra Fría.

De acuerdo con Benítez, la seguridad nacional de México ha tenido grandes incertidumbres respecto a su formulación, y le adjudica tres factores principales; el primero habla sobre la integración tardía a las tendencias mundiales y los procesos de regionalización; el segundo tiene como eje el período de la transición política, el cual centra su atención en los problemas que generaron los cambios en las instituciones, dificultando la definición de amenazas y riesgos respecto a políticas gubernamentales para hacerles frente. Por último, señala que el régimen heredado del contexto de la «Revolución», hizo que las políticas de seguridad y

[301] "Ley de Seguridad Nacional", p. 2.
[302] Para efectos prácticos de esta investigación, en adelante se establecerá SNM para decir Seguridad Nacional de México.
[303] José Luis Piñeyro, Gabriela Barajas, "La seguridad nacional con Fox: avances analíticos, retrocesos reales", *Revista Foro Internacional*, (191-192), 2008, p. 211, http://bit.ly/2keeror

defensa se adaptaran lentamente a las nuevas condiciones internas y externas.[304] Tales situaciones han provocado ambigüedades en la definición del concepto en relación a las dinámicas internacionales y geopolíticas de México.

Por otra parte, asevera que hay una cuestión que prevalece en México y que no se ha modificado, la cual trata de cómo están compuestas las Fuerzas Armadas. Hay una tajante separación entre la Secretaría de la Defensa y la Secretaría de Marina, las cuales deben velar por la seguridad y defensa de México; no obstante, tienen atribuciones distintas. En ese tenor, la crítica de Benítez radica en que no existe una separación del espacio aéreo, es decir, la Fuerza Aérea no es autónoma, sino que está ligada con el Ejército, lo que dificulta su desarrollo.[305]

CUADRO 11. MODELOS DE LA SEGURIDAD NACIONAL EN MÉXICO (1950-2003).[306]

En la Guerra Fría	En los noventa	En el siglo XXI
El enemigo es externo y está definido por el Estado a partir de la identificación con las ideologías de izquierda.	El enemigo es interno y el Estado lo identifica a partir de su rebeldía y acciones armadas.	No hay identificación del concepto de enemigo, por lo que se sustituye por el de competencia de posiciones.
El disidente del sistema, por tanto, es definido también como enemigo, al que se asume incluso como contrario a la coalición y al partido oficial.	El disidente es incorporado y cooptado mediante espacios políticos, para los cuales opera la vía partidista.	El campo de lo político alcanza sus posiciones en la competencia electoral, por lo tanto, su capacidad de influencia está ligada a su capacidad de convocatoria.
La seguridad nacional recurre a aparatos de penetración y represión de los espacios tanto opositores como disidentes.	La seguridad nacional requirió del paulatino desplazamiento de las figuras tradicionales encargadas de esta misión.	Los aparatos de seguridad nacional reclaman ser instrumentos para conseguir y analizar información, en la búsqueda por anticipar escenarios de riesgo.
Se exacerba el nacionalismo revolucionario y se niega toda ideología ajena al mismo.	El nacionalismo revolucionario pierde su impacto, incluso como ideología oficial, y es sustituido por el lenguaje tecnocrático.	La pluralidad fundada en la tolerancia será la base para alcanzar consensos válidos; no podrá haber una sola ideología de

[304] Raúl Benítez Manaut, "La seguridad nacional en la indefinida transición: mitos y realidades del sexenio de Vicente Fox", *Revista Foro Internacional*, (191-192), 2008, p. 184, http://bit.ly/2kefpRy
[305] Ibíd, p. 186.
[306] Cuadro sustraído de Guillermo Garduño Valero, "Metodología de la estrategia y la seguridad nacional", en *La seguridad nacional de México. Debate actual*, coordinado por José Luis Piñeyro, México, 2003, pp. 84-85.

		Estado o de gobierno y, por tanto, supone espacio social de las ideas.
La seguridad nacional es entendida como defensas de las instituciones: presidencial, partidista y del bloque en el poder.	La seguridad nacional es confundida en su proyecto con la obediencia a la Constitución, a la institución presidencial y como apoyo al Plan Nacional de Desarrollo.	La seguridad nacional será definida como construcción de los actores sociales, por tanto identificará las bases del compromiso con la obediencia al orden social y a la ley justa.
La base orientadora de sus acciones se funda en la defensa del orden y de la tranquilidad pública.	La base orientadora es la negociación a fin de alcanzar consensos, donde el punto central es el mantenimiento del orden.	La base orientadora de sus acciones será la participación social, lo que supone niveles de competencia civil en la propuesta.

Para efectos de esta investigación, el cuadro anterior tiene como propósito identificar cómo ha evolucionado la seguridad nacional de México con base a tres períodos, la Guerra Fría; los años noventa; y el siglo XXI. En ese tenor, se puede visualizar la manera en que se ha modificado el objeto de referencia, de acuerdo a la circunstancia. Al inicio de la Guerra Fría, y al término de la misma, se puede identificar la gran influencia del paradigma realista en las Relaciones Internacionales, pues el escenario de ese entonces, sólo perfilaba como amenazas y riesgos, las actividades hostiles de otros Estados.

A partir del fin de la Guerra Fría surgieron nuevas amenazas que no solamente provenían de las fuerzas militares de otro Estado, sino que su naturaleza distinta a cuestiones políticas las hace un constante riesgo para la sociedad civil.

Por lo tanto, es preciso destacar lo siguiente:

- «En la doctrina militar contemporánea, debido a que el "enemigo" no es ni externo ni una fuerza militar convencional, entonces es un enemigo irregular de baja intensidad y las fuerzas armadas mexicanas se enfrentan a actores no estatales que han rebasad las capacidades de los aparatos de seguridad pública e inteligencia civiles. Son enemigos no convencionales».[307]

En ese sentido, las definiciones teóricas y conceptuales en dicha materia tienen que adaptarse a las circunstancias de cierto espacio-tiempo. Se debe entender que, las amenazas como el crimen organizado, el terrorismo y otros grupos delictivos, también

[307] Presentación Raúl Benítez Manaut en Marcos Pablo Moloeznik, "Tratado sobre pensamiento estratégico-militar (Enseñanzas para el Sistema de Defensa de México)", *CASEDE*, 2018, p. xii, http://bit.ly/2mbjwOU

utilizan las Tecnologías de la Información y la Comunicación (TIC) para favorecer sus intereses, de modo que, se fortalecen y generan asimetrías con las instituciones gubernamentales encargadas de la seguridad y defensa.

La coyuntura innovadora de la Cuarta Revolución Industrial y el proceso de la globalización, han hecho que los fenómenos tradicionales de riesgos y amenazas tengan menos amplitud y discusión en los debates sobre seguridad; sin embargo, esto no quiere decir que no sigan representando un peligro potencial. Es en este contexto que «la complejidad y los nuevos problemas de seguridad vienen dados por un conjunto de factores tales como la ausencia de un enemigo geográficamente localizado, la existencia de adversario potenciales difíciles de identificar, la aparición de amenazas que no son de carácter militar, y que requieren respuestas no tradicionales».[308]

Se han generado diversas críticas a la actual SNM, debido a que no cuenta con los sustentos necesarios para afrontar las nuevas dinámicas del siglo XXI. En esa tesitura, De Miguel puntualiza que «… la actual Ley del año 2005 adolece… de un enfoque integral.»[309] Esto representa un argumento válido, pues la última reforma que se le realizó fue en ese mismo año. Por lo tanto, es necesario reflexionar y generar un debate sobre si sus fundamentos jurídicos aún sirven para afrontar los nuevos riesgos de naturaleza variable.

Con base en lo anterior, Rosales precisa lo siguiente:

> Este esfuerzo reconceptualizador…, conlleva la posibilidad de disminuir los errores tradicionales en la teoría, que tienen costos altos en la práctica, por su desfase de atender problemas en el funcionamiento de la gobernabilidad y en la demanda para resolver necesidades, intereses y deseos de la sociedad. [Además, la]… definición jurídica mexicana actual, registrada en la Ley de Seguridad Nacional vigente y otros documentos… rectores en la materia, obliga a repensar, desde su origen conceptual, jurídico y político, un nuevo alcance… de Seguridad Nacional…[que] incida en [la creación de una] Política de Estado. [De este modo]… se debe impulsar una reflexión a fondo, amplia y sistemática, de que nuestras viejas categorías espacio-temporales han cambiado con el desarrollo tecnológico, [por lo que

[308] Ibid, p. 466.

[309] Jesús De Miguel, "Reflexiones sobre la ley de seguridad nacional", *ININVESTAM*, Documento de Opinión, DO. 11/16, México, 2016, p. 2, http://bit.ly/2lHirhF

> se deben] revalorar las posibles sustituciones, [para entender] el impacto desde lo global y en lo local.[310]

El caso de la ciberseguridad tiene un carácter global, así como una dimensión interna que puede perjudicar los sistemas de información de las infraestructuras críticas de un Estado. Si éstas se ven afectadas por intrusiones cibernéticas, pueden poner en riesgo la estabilidad del gobierno, y con ello, comprometer la seguridad nacional. Por lo tanto, la SNM está ampliamente relacionada con la seguridad cibernética, puesto que gran parte de la innovación tecnológica se adapta a diversos sectores, especialmente, los que se encargan de la seguridad y defensa del Estado, así como los que cumplen un rol estratégico en la gestión y administración de la información.

Parte de las características del entorno virtual es que no se tienen fronteras estrictamente establecidas, de modo que, un ataque cibernético se puede desarrollar en cualquier parte del planeta, y por ende, su objetivo consista en afectar los sistemas operativos de empresas e instituciones gubernamentales.

La planeación y ejecución de un ciberataque puede ser desarrollado por miembros del crimen organizado que tengan como ideal sustraer dinero o información, grupos terroristas que busquen realizar ataques a infraestructuras críticas, *hackers* con motivaciones individuales, o bien, por Estados que pretendan ampliar su interés nacional a través del ciberespacio. Por lo tanto, la redefinición conceptual de la amenaza, riesgo y enemigo en el contexto de la Cuarta Revolución Industrial, podría establecer un marco de acción encaminado a modificar los esquemas de conflicto y confrontación tradicionales, puesto que los factores del tiempo y la innovación tecnológica digital, hacen posible que cambien rápidamente.[311]

A su vez, la falta de una Política de Estado resta margen operativo a las autoridades en el combate a ciertos riesgos y amenazas, debido a que, en cada nueva administración, se desarrollan nuevos objetivos de atención a ciertos factores de riesgo, por lo que no se

[310] Emilio Vizarretea Rosales, "Nueva inteligencia y ciberseguridad", *Revista del Centro de Estudios Navales*, vol. 37, 2016, pp. 51-52, http://bit.ly/2lNMm7C

[311] Guillermo Garduño, "Metodología de la estrategia y la seguridad nacional", en *La Seguridad Nacional en México…*, coordinado por José Luis Piñeyro, p. 79.

establece una política permanente que atienda los intereses del Estado en materia de seguridad nacional.

El establecimiento de una Política de Estado le ayudaría a México a concretar un nuevo modelo de seguridad nacional que trascienda el plano sexenal y se convierta en una hoja de ruta a seguir en el corto, mediano y largo plazo, de acuerdo a su condición geopolítica y a los fenómenos internacionales más relevantes. En tal sentido, se entendería que la seguridad nacional debe ser una constante de estudio y desarrollo permanente.

Es indispensable considerar lo anterior, debido a que es necesario tener una perspectiva global de los acontecimientos mundiales con el fin de establecer políticas y estrategias que permitan plantear nuevos enfoques de pensamiento en la dimensión de la seguridad nacional de México.[312] Por lo tanto, una Política de Estado en estrecha relación con la Agenda Nacional de Riesgos, permitiría identificar algunos escenarios que pudieran ocasionar inestabilidad y crisis a futuro.

Ante esto, es un requisito fortalecer la labor de las agencias encargadas de la generación de inteligencia estratégica, pues a partir de sus análisis, se pueden crear metas y objetivos para desarrollar a futuro. En ese sentido, Curzio agrega:

> Lo que México necesita es desarrollar agendas con alcances y horizontes específicos. [De modo que es prioritario]… establecer una diferencia sustantiva entre la agenda de seguridad estratégica (que engloba los temas que le dan viabilidad al país en el largo plazo) y la agenda táctico-operativa (que atiende las amenazas del aquí y el ahora).[313]

No obstante, la deficiencia de no tener horizontes específicos hace que el país se estanque en el desarrollo de una política de vanguardia que englobe agendas con alcances y horizontes específicos. La mayor parte de los ejes de acción tienen propósitos cortoplacistas, los cuales se basan en el Plan Nacional de Desarrollo y los respectivos programas que deriven como complemento del mismo.

Aunado a lo anterior, es indispensable visualizar la Seguridad Nacional de México como un factor de desarrollo para que se alinee a los intereses nacionales. La definición del interés

[312] Guadalupe González, "Una perspectiva global para la Seguridad Nacional de México", *Revista de Administración Pública*, vol. L, n. 1, 2015, p. 279, http://bit.ly/2lKeDMB
[313] Curzio, *La seguridad nacional de México…*, p. 90.

nacional tiene una estrecha interrelación con la Seguridad Nacional del país, debido a que sirve como instrumento disuasorio cuando se proyecta el Poder Nacional de México al interior y el exterior. Sin embargo, su aplicación dependerá de la categorización que determinado gobierno electo estipule en las políticas gubernamentales de su gestión.

Otro punto que es indispensable considerar consiste en fortalecer las instituciones estatales, las cuales tienen que ser tomadas en cuenta a partir de un enfoque integral, con el fin de dinamizar la cooperación e intercambio de información entre secretarías, para el mantenimiento del orden público en México. A su vez, los sectores de la seguridad y defensa no son los únicos que deben incrementar sus capacidades en materia de ciberseguridad, también es necesario que lo hagan áreas alternas, como la energética, la económica, la de salud, la de comunicaciones, entre otras. Por lo tanto, toda seguridad debe ser integral[314] para que tenga un resultado más efectivo, de lo contrario, un punto ciego o débil puede crear vulnerabilidades.

En ese sentido, Bandala menciona que:

> […] la política de Seguridad y Defensa del Estado mexicano, debe establecer la orientación del quehacer nacional para actuar ante potenciales amenazas, tanto externas como internas, que incluya sus niveles de aplicación, ya sea estratégico u operacional y de esta forma, [puedan] definir con claridad cuál será el actuar del país ante las distintas situaciones de crisis que afecten a su seguridad, fomentando además el incremento de las capacidades estratégicas para que se conviertan en un factor de disuasión que, aunado a una firme voluntad política, prevengan el escalamiento de una crisis que desemboque en un conflicto mayor y de esta forma [permitan] proteger los intereses y objetivos nacionales.

Por todo lo mencionado, es evidente que México carece de un enfoque multidimensional de la seguridad, toda vez que aún existen sectores que faltan ser cubiertos de manera integral, de modo que hace falta redoblar esfuerzos en materia de Seguridad Nacional. Actualmente, existen diversos puntos ciegos que pueden crear vulnerabilidades, especialmente, si se consideran los siguientes factores:

[314] Integral se refiere a que la seguridad debe estar bien distribuida a efecto de que las vulnerabilidades sean menores. En tal sentido, sería ideal partir de una política de seguridad en el ciberespacio (Ley General de Ciberseguridad) que haga obligatorio establecer estándares de enseñanza, protección y desarrollo de medidas de seguridad en el ciberespacio. Lo integral se visualiza en que la ciberseguridad debe estar presente en diversas áreas, tales como la energética, la financiera, en lo educativa, en las comunicaciones, entre otras.

- Ley de Seguridad Nacional no actualizada al contexto tecnológico;
- falta de visión a mediano y largo plazo en materia de seguridad nacional;
- cambio de políticas y estrategias debido a la gestión sexenal;
- falta de una Política de Estado con objetivos permanentes;
- separación o elaboración de una Ley propia de Seguridad Nacional, toda vez que en la Ley de Seguridad Nacional se mezcla la seguridad con la elaboración de inteligencia;
- y la no existencia de una política o ley que, tenga por objetivo, fortalecer las capacidades de acción y cooperación entre las instituciones que componen la seguridad nacional de México en materia de ciberseguridad.

Dichos criterios deben ser considerados como factores de riesgo, toda vez que para lograr una efectiva defensa, es prioritario anticipar las eventualidades que pudieran causar inestabilidad en la gobernabilidad del país, por lo tanto, lo mejor es fortalecer de manera permanente y gradual la seguridad nacional de México.

En ese sentido, las variables tecnológicas y el aumento paulatino por ataques cibernéticos, pueden causar efectos negativos en la seguridad nacional del país, especialmente si se sigue careciendo de los factores anteriormente mencionados.

Complementado lo anterior, De Miguel estipula lo siguiente:

> En el nuevo paradigma de la seguridad, dominado por la complejidad y la incertidumbre, las fuerzas armadas siguen teniendo un papel determinante no solamente en la defensa, sino en el modelo ampliado de la seguridad, y para ello se requiere que estén en permanente transformación, para que de ésta forma, tener la capacidad de adaptarse a los escenarios cambiantes que exige la seguridad del siglo XXI.[315]

La integración del ciberespacio a la Ley de Seguridad Nacional permitiría tener como base, la creación de nuevas políticas y estrategias que tengan como propósito dar certidumbre jurídica a las acciones de futuras administraciones de gobierno. Por lo tanto, se daría un mayor margen de maniobra a la recién creada Estrategia Nacional de Ciberseguridad, debido a que toda estrategia requiere de los suficientes elementos jurídicos para que sea

[315] Jesús De Miguel, "La Seguridad Nacional y la gran estrategia", *ININVESTAM*, Documento de Análisis, DA. 50/18, 2018, p. 16, http://bit.ly/2mc6qkB

funcional.[316] A su vez, también se destinaría un presupuesto para abordar el tópico en cuestión.

El Plan Nacional de Desarrollo y el Programa para la Seguridad Nacional de la administración 2013-2018, desarrollaron un modelo de seguridad con una perspectiva multidimensional, por lo que se podría tomar como un referente para el establecimiento futuro de una Política de Estado que englobe y fortalezca el plano de la seguridad, especialmente el que hace referencia a la Seguridad Nacional de México en relación con la ciberseguridad.

5.2 Gestión sexenal en materia de ciberseguridad 2013-2018

Para efectos de esta investigación se tomó como referencia la gestión de la administración del ex Presidente Enrique Peña Nieto en el tema de la seguridad nacional y la ciberseguridad, para identificar cuáles fueron los avances en tales materias, por lo anterior, se toman en cuenta el Plan Nacional de Desarrollo (2013-2018), el Programa para la Seguridad Nacional (2014-2018) y los Informes de Gobierno (2012-2018), puesto que son evidencia práctica de lo que se hizo y de lo que falta por hacer.

5.2.1 Plan Nacional de Desarrollo (2013-2018)

En la Constitución Política de los Estados Unidos Mexicanos se estipula, en su artículo 26, que se debe crear un Plan Nacional de Desarrollo (PND) para determinar las oportunidades que la nación requiera, así como los riesgos que debe afrontar. A partir de ello, se creará un documento en donde se enmarcarán los lineamientos generales de las políticas públicas del nuevo gobierno. Además, señala:

> La ley facultará al Ejecutivo para que establezca los procedimientos de participación y consulta popular en el sistema nacional de planeación democrática, y los criterios para la formulación, instrumentación, control y evaluación del plan y los programas de desarrollo. Asimismo, determinará los órganos responsables del proceso de planeación y las bases para que el Ejecutivo Federal coordine, mediante convenios, con los gobiernos de las entidades federativas e induzca y concierte con los particulares, las acciones a realizar para su elaboración y ejecución. El plan nacional de desarrollo considerará la continuidad y adaptaciones necesarias de la política nacional para el desarrollo industrial, con vertientes sectoriales y regionales.[317]

[316] La estrategia es una herramienta, pero necesita de una Ley que le dé fundamento.
[317] "Artículo 26", *Orden Jurídico,* acceso el 10 de octubre de 2018 en: http://bit.ly/2kalvCj

De acuerdo a la Ley de Planeación, el artículo 21, establece que el Presidente debe remitir el Plan Nacional de Desarrollo a la Cámara de Diputados del Congreso de la Unión para que sea aprobado. Además, se precisa que la vigencia del Plan no debe exceder el plazo del gobierno sexenal. Por otra parte, menciona que se debe tomar en cuenta la creación de objetivos generales a largo plazo con las consideraciones y proyecciones de por lo menos veinte años. Aunado a lo anterior, resalta:

> El Plan Nacional de Desarrollo precisará los objetivos nacionales, la estrategia y las prioridades del desarrollo integral, equitativo, incluyente, sustentable y sostenible del país, contendrá previsiones sobre los recursos que serán asignados a tales fines; determinará los instrumentos y responsables de su ejecución, establecerá los lineamientos de política de carácter global, sectorial y regional; sus previsiones se referirán al conjunto de la actividad económica, social, ambiental y cultural, y regirá el contenido de los programas que se generen en el sistema nacional de planeación democrática.[318]

Además, en la Ley de Seguridad Nacional, en su artículo 7, se establece que en el Plan Nacional de Desarrollo se tienen que definir temas de Seguridad Nacional y, a su vez, para elaborar la Agenda Nacional de Riesgos, se debe tener en cuenta el PND.

En lo referente a seguridad nacional, el PND 2013-2018, menciona:

> El concepto jurídico de Seguridad Nacional condensa una serie de objetivos e intereses estratégicos nacionales, tales como la protección de la nación mexicana frente a las amenazas y riesgos; la preservación de la soberanía e independencia nacionales y la defensa del territorio; el mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno; la preservación de la unidad de las partes integrantes de la Federación; la defensa legítima del Estado Mexicano respecto de otros Estados o sujetos de derecho internacional; y el desarrollo económico, social y político del país como ejes en la preservación de la democracia.[319]

El PND 2013-2018, se basa en la Ley de Seguridad Nacional para retomar el concepto de seguridad nacional. Además, reconoce que la naturaleza de los problemas y desafíos tienen una tendencia cambiante, de modo que retoma un modelo de seguridad más amplio y multidimensional para fortalecer el proyecto nacional.

En el capítulo «Objetivos, estrategias y líneas de acción» del PND, el objetivo 1.2., consiste en garantizar la seguridad nacional. Para llevar a cabo dicho propósito, se creó la estrategia

[318] "Ley de Planeación", *Cámara de Diputados del H. Congreso de la Unión*, acceso el 10 de octubre de 2018 en: http://bit.ly/2lK4W0u

[319] "Plan Nacional de Desarrollo 2013-2018", *Gobierno de la República*, 2013, p. 31, http://bit.ly/2ktKd0U

1.2.3., que pretende fortalecer la inteligencia del Estado mexicano para contrarrestar las amenazas. Las líneas de acción estipulan la manera en cómo se llevarán a cabo los dos criterios anteriores, de modo que se destacan las tres siguientes por su interrelación en el ámbito de la seguridad nacional y el ciberespacio:

> Impulsar, mediante la realización de estudios e investigaciones, iniciativas de ley que den sustento a las actividades de inteligencia civil, militar y naval, para fortalecer la cuarta dimensión de operaciones de seguridad: ciberespacio y ciberseguridad;
> Coadyuvar en la identificación, prevención, desactivación y contención de riesgos y amenazas a la Seguridad Nacional, y;
> Diseñar e impulsar una estrategia de seguridad de la información, a efecto de garantizar la integridad, confidencialidad y disponibilidad de la información de las personas e instituciones públicas y privadas en México.[320]

5.2.2 Programa para la Seguridad Nacional

Derivado del Plan Nacional de Desarrollo, se elaboró el Programa para la Seguridad Nacional 2014-2018 con el objetivo de delinear el contexto de las amenazas y riesgos que pueden perjudicar los intereses de México de acuerdo a la meta sexenal. En este sentido, el programa enmarca dos objetivos estratégicos que se interrelacionan con los objetivos del PND 2013-2018 en lo que concierne a seguridad nacional, siendo estos:

> Consolidar el Sistema de Seguridad Nacional mediante el desarrollo y articulación permanente de los sistemas y procesos de los que dispone el Estado mexicano para asegurar la atención integral de las vulnerabilidades, los riesgos y las amenazas a la Seguridad Nacional. [Y por otra parte] Asegurar que la política de Seguridad Nacional del Estado mexicano adopte una perspectiva multidimensional mediante la coordinación de las autoridades e instituciones competentes, para favorecer la consecución de los objetivos e intereses nacionales.[321]

En el tercer apartado «Modelo de Seguridad Nacional», se hace mención de que la política de seguridad nacional de la administración del ex presidente Enrique Peña Nieto, buscó promover el desarrollo nacional y de seguridad del Estado mexicano para fortalecer el

[320] Ibíd., p. 107.
[321] "Programa para la Seguridad Nacional 2014-2018. Una Política Multidimensional para México en el siglo XXI", *Presidencia de la República*, 2014, p. 32, http://bit.ly/2mab8PF

Sistema de Seguridad Nacional, considerando las instituciones encargadas de la defensa exterior, seguridad interior y protección civil.[322]

El cuarto apartado «Posición de México en el mundo», en materia de ciberseguridad, señala lo siguiente:

> El Plan Nacional de Desarrollo 2013-2018 dispone el fortalecimiento de las capacidades institucionales en el ciberespacio y la ciberseguridad. Los delitos de suplantación de identidad, fraudes financieros, distribución de pornografía infantil, entre otros, han prosperado en el ciberespacio generando un alto costo económico y humano. En este sentido, surge la necesidad de concentrar esfuerzos y recursos para combatir el ciberdelito e impulsar una legislación en la materia a nivel nacional. De igual modo, resulta prioritario fortalecer la cooperación internacional, en particular con América del Norte, con el fin de identificar, prevenir y contener los riesgos y amenazas a la Seguridad Nacional que provengan del ciberespacio.[323]

De manera específica, se detallan los principales delitos que han causado estragos económicos y sociales; además, se fundamenta la necesidad de legislar a nivel nacional en lo referente al ciberdelito. Por otra parte, la Teoría de Complejos de Seguridad Regional está presente cuando se enuncia el tema de la cooperación internacional, haciendo énfasis en la región de América del Norte como mecanismo para identificar riesgos comunes, y con ello, preservar la seguridad nacional. De este modo, la agenda del ciberespacio se visualiza como un intento regional para securitizar la ciberseguridad desde el enfoque multidimensional de la seguridad.

Con base en lo anterior, el sexto apartado «Riesgos y Amenazas», sitúa 5 factores de riesgo que pueden ocasionar inestabilidad en el Estado mexicano. El primero destaca los desastres naturales y pandemias; el segundo, la delincuencia organizada transnacional; el tercero, la ciberseguridad; el cuarto, las fronteras, mares y flujos migratorios irregulares, y el quinto, el terrorismo y las armas de destrucción masiva. En ese tenor, el asunto de la seguridad cibernética destaca que la poca existencia de una cultura de seguridad de la información, representa una vulnerabilidad en el país; de modo que se debe fortalecer la cuarta dimensión de operaciones en dicha materia para atenuar los efectos negativos.[324]

[322] Ibíd., p. 37.
[323] Ibíd., p. 54.
[324] Ibíd., p. 64.

Los objetivos, estrategias y líneas de acción que se encuentran en el Programa, se pueden visualizar en el siguiente cuadro.

CUADRO 12. OBJETIVOS, ESTRATEGIAS Y LÍNEAS DE ACCIÓN DEL PROGRAMA PARA LA SEGURIDAD NACIONAL 2014-2018.[325]

Objetivos	Estrategias	Líneas de acción
2.1. Definir anualmente una Agenda Nacional de Riesgos con carácter multidimensional, para promover la atención integral de los temas de Seguridad Nacional mediante el desarrollo de acciones conjuntas a fin de hacer frente a riesgos y amenazas.	2.1.2. Desarrollar una política de Estado en materia de seguridad cibernética y ciberdefensa, para proteger y promover los intereses y objetivos nacionales.	2.1.2.1. Impulsar proyectos normativos que regulen esquemas de seguridad de la información homólogos en todos los sectores del país, para prevenir y enfrentar ataques cibernéticos; 2.1.2.2. Designar la unidad administrativa encargada de emitir, evaluar e impulsar el cumplimiento de la política de seguridad cibernética y ciberdefensa para el Ejecutivo Federal; 2.1.2.3. Fortalecer los mecanismos de coordinación para la atención a incidentes de seguridad cibernética en el ámbito del Ejecutivo Federal; 2.1.2.4. Impulsar el cumplimiento y el desarrollo de procedimientos para evaluar y fortalecer el funcionamiento de los equipos de respuesta a incidentes de seguridad cibernética en el ámbito del Ejecutivo Federal; 2.1.2.5. Fortalecer las capacidades humanas, tecnológicas y la infraestructura para atender incidentes de seguridad cibernética; 2.1.2.6. Establecer esquemas de cooperación internacional en materia de seguridad cibernética y ciberdefensa para prevenir y enfrentar ataques a los sistemas informáticos del país.
	2.2.6. Fomentar la preparación del personal militar y naval, así como la mejora continua del sistema de formación y	2.2.6.7. Incrementar la capacitación y el adiestramiento del personal militar y naval en materia de inteligencia,

[325] Cuadro extraído del Programa para la Seguridad Nacional 2014-2018. Una política multidimensional para México en el siglo XXI.

	educación de las Fuerzas Armadas.	contrainteligencia, ciberseguridad y ciberdefensa.

El anterior cuadro ejemplifica la relación entre el PND y la Agenda Nacional de Riegos, los cuales deben ser tomados en cuenta para la consecución de los intereses de la nación respecto a la seguridad nacional. La estrategia 2.1.2 es ambiciosa, sin embargo cabe destacar que el establecimiento de una Política de Estado en materia de ciberseguridad tiene que ser gradual y debe contar con el respaldo de otros actores en el plano nacional, tales como el sector privado, la academia, la sociedad civil, y en el ámbito público, el poder judicial, legislativo y ejecutivo. Respecto a las líneas de acción, tienen sentido si se toma en cuenta el corto y mediano plazo de la administración, por lo que corresponderá nuevos gobiernos darle continuidad a largo plazo, siendo el más próximo el de Andrés Manuel López Obrador.

5.2.3 Informes de Gobierno

En el Primer Informe de Gobierno 2012-2013, para garantizar la Seguridad Nacional, se incorporó el enfoque multidimensional a la Agenda Nacional de Riesgos para ampliar los factores que pueden provocar vulnerabilidades en las actividades del país. En materia del ciberespacio, se generó un protocolo de colaboración entre el CERT-MX y las entidades que conforman el Consejo de Seguridad Nacional para salvaguardar las infraestructuras cibernéticas.[326]

Por otra parte, se mencionó el trabajo desarrollado por la SEMAR y la SEDENA en el ámbito del ciberespacio, destacando que la primera implementó un programa para comenzar con el desarrollo de capacidades mediante el soporte de la Comisión de Seguridad de la Información, para resguardar los archivos tanto en lo físico como en lo electrónico.[327] La SEDENA creó el «Programa para generar el desarrollo de la ciberdefensa en el Ejército y Fuerza Aérea Mexicanos», aunque se precisó que su estatus quedó sujeto a revisión y aprobación,[328] de modo que no entró en operaciones. Además, para tener un manejo más eficiente de los controles y medidas de seguridad de la información, se creó un registro actualizado de los enlaces de la Administración Pública Federal encargados de ejecutar el

[326] "Primer Informe de Gobierno", *Presidencia de la República*, 2013, p. 52, http://bit.ly/2lGch17
[327] Ibíd., p. 53.
[328] Ibíd.

Manual Administrativo de Aplicación General en materia de Tecnologías de Información, Comunicaciones y Seguridad de la Información (MAAGTICSI).[329]

El Segundo Informe de Gobierno 2013-2014, señaló las acciones que desempeñaron algunas instituciones como la SEMAR y la SEDENA en lo referente a la cuarta dimensión de operaciones.

Las actividades[330] más relevantes para la SEDENA fueron la participación y asistencia de personal a talleres, reuniones y otros eventos. Del 15 al 21 de septiembre del año 2013, participó en el seminario *Ciber Endeavor*, auspiciado por el Comando Norte de los Estados Unidos (*USNORTHCOM*, por sus siglas en inglés) en Alemania. Además, el 14 del mismo mes, designaron a un representante ante la OEA para cumplir la función de gerente en el Programa en Seguridad Cibernética del Comité Interamericano contra el Terrorismo (CICTE).[331]

En lo que respecta a la SEMAR, realizó, en coordinación con el Comando Norte de Estados Unidos, el Taller Técnico de Ciberseguridad, así como también modernizó y reestructuró el Centro de Monitoreo y Respuesta a Incidentes de Seguridad en el Ciberespacio. Además, en conjunto con la SEDENA, desarrollaron el Protocolo de Colaboración para el Intercambio de Información Relacionada con la Ciberdefensa, Ciberseguridad y Seguridad de la Información en el Ciberespacio.[332] Por último, y dando seguimiento a la seguridad de la información, se actualizó el MAAGTICSI.

Lo anterior demuestra la colaboración existente con la región de América del Norte, al llevar a cabo acciones conjuntas con el Comando Norte. Por otra parte, la designación del representante ante la OEA resulta importante para México, porque es la organización que trata temas de seguridad desde una perspectiva multidimensional, en el que destaca el tema de la ciberseguridad.

[329] El MAAGTICSI tiene como objetivo definir los procesos con los que, en TIC y Seguridad de la Información, las instituciones deben regular su operación independientemente de su estructura organizacional y las metodologías con las que dispongan. "¿Qué es MAAGTICSI?", *Secretaría de Desarrollo Agrario, Territorial y Urbano*, acceso el 11 de octubre de 2018 en: http://bit.ly/2kr48NX

[330] Las actividades son diversas, sin embargo, se enlistan las más importantes para los propósitos de esta investigación.

[331] "Segundo Informe de Gobierno", *Presidencia de la República*, 2014, p. 57, http://bit.ly/2k8X7kw

[332] Ibíd.

El Tercer Informe de Gobierno 2014-2015, destacó la importancia del Centro de Estudios Superiores Navales (CESNAV), por la realización del seminario «Seguridad y Defensa en el Ciberespacio», el cual, estructuró la relevancia del ciberespacio en la seguridad nacional.[333] La SEMAR, llevó a cabo, de manera conjunta con el Comando Norte de los Estados Unidos, seminarios, cursos y conferencias; aumentando más su participación con ese organismo.

Por otra parte, se señala que la SEGOB participó en la actualización de dos asuntos, la Estrategia de Seguridad de la Información y el Protocolo de Colaboración entre el CERT-MX y las instancias de seguridad nacional.[334] Además, se trabajó en la creación de un Catálogo de Infraestructuras Críticas de Información en el Gobierno Federal, de modo que se le dio continuidad a las labores anteriores

Las acciones de la SEDENA consistieron en la participación de dos eventos importantes; el primero fue la «Primera Ronda de Conversaciones en Temas de Ciberdefensa con el Comando Conjunto de las Fuerzas Armadas de Perú». El segundo fue con el Ministerio de Defensa de Israel, en el «Cuarto Seminario de Seguridad Interior, Conferencia en materia de Defensa, Inteligencia, Ciberseguridad y Sistemas de Prisiones». Por otra parte, en el marco del Grupo Bilateral de Cooperación en Seguridad México-Estados Unidos de América, la SEDENA se integró al Subgrupo de Seguridad Cibernética de dicha instancia.[335]

El Cuarto Informe de Gobierno 2015-2016, mostró más resultados en el ámbito de la ciberseguridad. En ese sentido, hubo un incremento en la atención del tópico por parte de México a nivel nacional e internacional.

En lo que respecta a los acontecimientos mundiales, México fue participe de un gran número de eventos, de los cuáles, se pueden destacar los siguientes:[336]

- Ejercicio Internacional CyberEx: se realizó en España y contó con la participación remota del CERT-MX para identificar la capacidad de resiliencia de los sectores que pueden tener mayor impacto en la seguridad nacional.

[333] "Tercer Informe de Gobierno", *Presidencia de la República,* 2015, p. 52, http://bit.ly/2lGcv8t
[334] Ibíd.
[335] Ibíd.
[336] "Cuarto Informe de Gobierno", *Presidencia de la República*, 2016, p. 83, http://bit.ly/2lL58N1

- Conferencia Meridian: se desarrolló en España y el objetivo fue la cooperación de ideas y experiencias de las entidades gubernamentales que se encargan de las infraestructuras críticas de información.
- Asistencia a la decimocuarta Sesión del Comité del Convenio sobre la Ciberdelincuencia: se llevó a cabo en Francia y la misión de México consistió en evaluar la posible aplicabilidad en el país.
- Entrenamiento Internacional de Ciberseguridad: se desarrolló en Estados Unidos y el objetivo consistió en instruir a sujetos que se encargan de realizar investigaciones sobre cibercrimen y ciberdelincuencia.
- Escuela del Sur de Gobernanza de *Internet*: se realizó en Estados Unidos y contó con la participación de personal de la SEDENA.
- Intercambio de experiencias y buenas prácticas en ciberseguridad: los trabajos se llevaron a cabo en España y Estonia con apoyo de la Organización de los Estados Americanos.
- Octavo Foro Internacional sobre Ciberseguridad: la sede fue Francia y asistió la Procuraduría General de la República (PGR) para intercambiar ideas sobre soberanía y seguridad en el ciberespacio.

Por otra parte, para fortalecer la Administración Pública Federal, se impulsó una estrategia para concienciar a los servidores públicos de alto nivel, con el fin de homologar los conocimientos en ciberseguridad en diversas entidades e instituciones.

Las acciones de la SEMAR fueron variadas, sin embargo, es prioritario destacar la Séptima Reunión de Estados Mayores México-Francia, que consistió en fortalecer el plan de colaboración entre ambos países para el intercambio de información sobre las amenazas cibernéticas.

La SEDENA realizó diversas actividades, entre las que destacan, su participación en el ejercicio de gabinete multinacional PANAMAX 2016, organizado por las Fuerzas Armadas de los Estados Unidos; esto permitió adquirir experiencia en operaciones combinadas. Por otra parte, en ese mismo año, se llevó a cabo, en instalaciones de la SEDENA, el Ejercicio de Gabinete CYBERLIBERTAD 2016, en el que participaron diversas instancias de seguridad nacional (SRE, SEMAR, CISEN, SCT) e instituciones académicas (UNAM e IPN),

además de una delegación compuesta por las Fuerzas Armadas, entidades académicas y dependencias gubernamentales de los Estados Unidos, con el objetivo de desarrollar una comprensión mutua, así como delimitar las funciones y responsabilidades en el área de la ciberseguridad.[337]

En ese orden de ideas, con base en el PND y el Programa Sectorial de la SEDENA, se creó el Centro de Operaciones del Ciberespacio para identificar y mitigar las amenazas que se encuentran en el ciberentorno, y que pueden comprometer las infraestructuras críticas de México. Además, el informe señaló que el MAAGTICSI no sólo fue actualizado, sino que, se reformó para tener una mejor implementación en la Administración Pública Federal.

A diferencia de los anteriores informes donde Estados Unidos era la única referencia para la cooperación; en esta evaluación, Francia y España adquieren un mayor dinamismo de colaboración con México en materia de seguridad cibernética. Por lo tanto, el Estado mexicano logró diversificar sus horizontes de trabajo en conjunto con naciones que desarrollan el tema de la ciberseguridad desde distintos ámbitos.

El Quinto Informe de Gobierno 2016-2017, destacó las actividades de la SEMAR, PGR y SEDENA en materia de ciberespacio, teniendo en consideración su participación en seminarios, talleres, conferencias, entre otros.

La SEDENA participó en el Ejercicio de Gabinete PANAMAX 2017, en Estados Unidos y Panamá. Además, llevó a cabo el quinto Seminario de Seguridad Interior y Cyber-Seguridad en la Ciudad de México. Aunado a esto, también realizó el «Taller Hacia una Estrategia Nacional de Ciberseguridad»,[338] sentando las bases introductorias para la elaboración de dicha estrategia.

La PGR asistió a la XXIV Asamblea General de la Asociación Iberoamericana de Ministerios Públicos, lo que dio origen a la Red Iberoamericana de Fiscales Especializados en Ciberdelincuencia. En un sentido similar, participó en el «Taller Avanzado Regional de Capacitación en Delito Cibernético para Fiscales», dando seguimiento a los trabajos auspiciados por la OEA.

[337] Ibíd., p. 85.
[338] "Quinto Informe de Gobierno", *Presidencia de la República*, 2017, p. 79, http://bit.ly/2lL5a7B

En otra tesitura, la SEMAR creó la Unidad de Ciberseguridad (UNICIBER), que depende del Estado Mayor General de la Armada; siendo su objetivo, planear y ejecutar actividades de ciberseguridad, ciberdefensa y seguridad de la información para proteger la infraestructura crítica de la institución. También participó en el Ejercicio de Gabinete Cyber Libertad Américas 2017, donde asistieron miembros del Comando Norte de los Estados Unidos, Brasil y Colombia.[339]

También establecieron dos criterios importantes que fueron eventos base para la elaboración de la Estrategia Nacional de Ciberseguridad. La Comisión Nacional de Seguridad y la Policía Federal, en coordinación con la OEA, llevaron a cabo la Segunda Semana de Ciberseguridad, además de que también dieron inicio a la campaña Ciberseguridad México 2017.

El Sexto Informe de Gobierno 2017-2018, es el último del sexenio de Enrique Peña Nieto. Aquí se pueden identificar los avances y la evolución que ha tenido el asunto de la seguridad en el ciberespacio.

Entre las acciones que llevó a cabo la SEDENA, se destacaron dos eventos en el ámbito operativo internacional, las «Jornadas de Ciberdefensa 2018, Operaciones Militares en el Ciberespacio» en España y el «Ejercicio C*yber Tradewinds* 2018», en las Bahamas.[340]

Por otra parte, la SEMAR participó en el Primer Ejercicio Iberoamericano de Ciberdefensa; además de que asistió al «Programa de Ciberseguridad, Centro Marshall, Alemania», para llevar a cabo análisis para el planeamiento y desarrollo de estrategias, con base a un entendimiento común.[341]

Es necesario tener como referente los Informes de Gobierno, puesto que es útil conocer los resultados en ciberseguridad durante la administración estudiada en dicha materia. Sin duda, son diversas las actividades que se desarrollaron en el sexenio del ex presidente Enrique Peña Nieto, aunque la mayoría se centra en reuniones y asistencia a eventos nacionales e internacionales, hay otros que se destacan por las acciones operativas como lo son el Ejercicio de Gabinete PANAMAX 2017 en Estados Unidos y Panamá, así como las Jornadas

[339] Ibíd.
[340] "Sexto Informe de Gobierno", *Presidencia de la Repúbica*, ,2018, p. 87, http://bit.ly/2lL5fbp
[341] Ibíd.

de Ciberdefennsa 2018 en España y el Ejercicio *Cyber Tradewinds* 2018 en Bahamas. Dichos ejercicios representan enormes oportunidades no sólo para aprender, sino para realizar autoevaluaciones sobre el nivel que tiene México respecto a otros países.

De todas las actividades, hay dos secretarías que tienen un rol fundamental para el desarrollo y progreso de la ciberseguridad, pero más aún en el rubro de la ciberdefensa, éstas son la Secretaría de la Defensa Nacional y la Secretaría de Marina. Entre las acciones que realizaron, destacan la creación del Protocolo de Colaboración para el Intercambio de Información Relacionada con la Ciberdefensa, Ciberseguridad y Seguridad de la Información en el Ciberespacio; también, por parte de la SEDENA, el establecimiento del Centro de Operaciones del Ciberespacio, y en lo que respecta a la SEMAR, la creación de la Unidad de Ciberseguridad, son resultados tangibles que sirven para dar fortaleza al tópico en cuestión.

Si se toma como base, lo realizado hasta el fin del sexenio puede ser funcional para estructurar y desarrollar mejores esquemas y protocolos en seguridad cibernética. La mayor parte de las actividades tuvieron como referente la asistencia a eventos internacionales en donde indudablemente se obtuvieron conocimientos al respecto. Por tal motivo, se vuelve una necesidad seguir siendo participe de las dinámicas internacionales en dicha materia, por dos sencillos factores; el primero consiste en que otros países identificarían a México como un Estado responsable, lo que le otorgaría al país un plus en el desarrollo del tema, permitiéndole asistir a más eventos similares; el segundo le daría a México la oportunidad de realizar ejercicios en conjunto con Estados más avanzados, creando la oportunidad de integrarse con algunos comandos especializados en dicha materia.

En ese tenor, la región predominante para México es América del Norte y, por obvias razones, en cuestión de seguridad compartida y teniendo en cuenta la relación bilateral, Estados Unidos es el principal país con el que se realizaron ejercicios y actividades en conjunto. Esto representa una ventaja para México porque puede adquirir muchos conocimientos técnicos y operativos.

Si bien es relevante seguir trabajando el tema con Estados Unidos, se debe tomar en cuenta que no se debe centrar toda la atención con el vecino del Norte, toda vez que hay países dispuestos a intercambiar información con México, por lo que sería oportuno establecer y

mantener un diálogo permanente con los siguientes países: España, Israel, Francia, Estonia, Canadá, Alemana, Corea del Sur, Uruguay, Brasil y Colombia. Se menciona a tales países porque se encuentran situados en diversas zonas geográficas del mundo y tienen una buena evaluación en dicho tópico, esto de acuerdo al Índice Mundial de Ciberseguridad.

5.3 Continuidad a la Estrategia Nacional de Ciberseguridad

Ya existía un precedente para la creación de la Estrategia Nacional de Ciberseguridad. En el año 2012, el Gobierno creó el Comité Especializado en Seguridad de la Información (CESI), que tenía por objetivo la elaboración de una Estrategia Nacional de Seguridad de la Información (ENSI).[342]

Con el propósito de que el país esté a la vanguardia en los avances tecnológicos, el gobierno del ex presidente Enrique Peña Nieto impulsó la creación de la Estrategia Digital Nacional (EDN), siendo muy similar a la que llevó a cabo la Unión Europea. Dicha estrategia articula las acciones que fomentan el desarrollo de infraestructura, haciendo posible el acceso de las TIC en el ámbito social, económico y político, para efectuar la transición hacia una era digital.

A nivel internacional, la prioridad y enfoque de los gobiernos consiste en crear sociedades de la información y el conocimiento para que exista un desarrollo más transparente, pero también más eficiente a nivel general y que esté al alcance de la mayoría. Por lo tanto, la EDN tiene por objetivo construir las bases para que México esté a la vanguardia en cuanto a tecnología digital se refiere, esto para que el país pueda alcanzar sus metas e intereses nacionales a través del desarrollo de las TIC.[343]

La EDN tiene 5 objetivos a cumplir:

> Transformación Gubernamental: Es la construcción de una nueva relación entre la sociedad y el gobierno, basada en la experiencia de los ciudadanos como usuarios de los servicios públicos.
>
> Economía digital: Es aquella en la que la asimilación de tecnologías digitales en los procesos económicos estimula el aumento de la productividad y el desarrollo de nuevas empresas, productos y servicios digitales.

[342] "Recomendaciones para el Desarrollo de la Estrategia Nacional de Ciberseguridad", *Organización de los Estados Americanos*, 2017, p. 6, http://bit.ly/2lHV5Ze

[343] "MéxicoDigital", acceso el 12 de octubre de 2018 en: http://bit.ly/2kb9xsa

> Educación de calidad: Este objetivo busca integrar y aprovechar a las TIC en el proceso educativo para insertar al país en la Sociedad de la Información y el Conocimiento.
> Salud universal y efectiva: Una política digital integral de salud implica aprovechar las oportunidades que brindan las TIC con dos prioridades: por una parte, aumentar la cobertura, el acceso efectivo y la calidad de los servicios de salud, y, por otra, usar más eficientemente la infraestructura instalada y recursos destinados a la salud en el país.
> Seguridad ciudadana: Este objetivo se refiere a la utilización de las TIC para promover la seguridad y para prevenir y mitigar los daños causados por los desastres naturales.[344]

Para su implementación, se requiere trabajar en los mecanismos de seguridad de la información para lograr un pleno desarrollo de las metas con el fin de mitigar los riesgos que puedan atentar contra los intereses de la nación. La idea es adaptar al país en el ámbito digital, pero para lograrlo, es necesario incrementar los niveles de seguridad en las infraestructuras y los sistemas informáticos.

En ese sentido, la Organización de los Estados Americanos ha ayudado a México en la elaboración de la Estrategia Nacional de Ciberseguridad (ENC). En el año 2017, emitió un documento denominado *Recomendaciones para el Desarrollo de la Estrategia Nacional de Ciberseguridad*, en el que explicó la situación del país, y con base en ello, realizó diversas recomendaciones para que el Gobierno de México las tuviera en cuenta para la elaboración de su estrategia. A continuación se especificarán algunos puntos derivados de las recomendaciones a fin de ilustrar los criterios que pueden ser relevantes para la actualización de la ENC, puesto que ya ha sido elaborada.

La OEA sugiere que la estrategia debe ser implementada por el más alto nivel de gobierno para que, al generar los objetivos a corto, mediano y largo plazo, y teniendo en cuenta las capacidades materiales e inmateriales, hagan posible una aplicación más eficiente. Además, se insta a que el gobierno considere la participación de diversos sectores para que la estrategia dé un resultado múltiple al conocer todas las variantes necesarias en su formulación.

Un área en la que México podría impulsar la inversión es en investigación y desarrollo. En este sentido, la OEA argumenta:

[344] "¿Qué es la Estrategia Digital Nacional?", Presidencia de la República, 17 de mayo de 2014, acceso el 12 de octubre de 2018 en: http://bit.ly/2lNkSzi

> México podría beneficiarse del desarrollo en las áreas de encriptación o autenticación (por ejemplo, biometría), servicios electrónicos o software/sistemas operativos. Sin embargo, dado que estas áreas aún no han sido identificadas como necesidades nacionales, no han recibido la misma atención en comparación con otras áreas de investigación.[345]

El desarrollo de esta recomendación incrementaría el potencial de México en la generación de sistemas operativos nacionales, debido a que el país es dependiente de componentes tecnológicos extranjeros.

Esto supone una debilidad estructural, pues aumenta la sujeción hacia materiales elaborados en otros países. En esa tesitura, Arreola enfatiza:

> México parece olvidar que ser dependiente de lo que otros hacen lo único que genera es mayor inseguridad; hay que recordar que la seguridad de individuos, organizaciones y estados radica en el secreto y en el dispositivo. Esto se logra a través del diseño y producción nacional de ciencia, tecnología, instrumentos, políticas, planos, estrategias e innovaciones, que sean desconocidas por los potenciales adversarios.[346]

Otra vulnerabilidad que tiene México es la falta de oportunidades laborales en seguridad cibernética debido a que algunas empresas no tienen en cuenta los riesgos que se encuentran en el ciberespacio; de modo que, es poca la demanda de personal especializado en tecnologías de la información y en seguridad de la misma. Esto implica dos cosas, la primera es que las compañías no cuentan con eficientes estándares de seguridad cibernética y lo segundo es causa de lo primero, pues al no contratar a personas especializadas que puedan proveer dicha seguridad, entonces el riesgo de padecer ataques cibernéticos se vuelve alto.

Aunado al párrafo anterior, a los egresados se les suele otorgar un puesto operacional, que no involucra el desarrollo de investigación e innovación, mermando categóricamente la capacidad del país en ese rubro. En este sentido, la recomendación de la OEA es «establecer iniciativas específicas para hacer crecer un mercado mexicano de seguridad cibernética».[347]

---

[345] "Recomendaciones para el Desarrollo…", p. 14.
[346] Arreola, *Ciberespionaje: la puerta al mundo…*, p. 191.
[347] "Recomendaciones para el Desarrollo…", p. 15.

Un asunto en el que se hace énfasis, es que se ha impulsado la inversión únicamente a nivel federal, descuidando a nivel estatal y municipal, lo referente a seguridad cibernética, provocando que los servicios sean deficientes en los dos últimos. Aunado a esto, un desafío para México consiste en establecer un marco legislativo y regulatorio que sea compatible con los tres niveles de gobierno para que se desarrolle un cumplimiento total en la estructura operativa. Esto supone una desventaja para el país si se toma en cuenta que los estados y municipios son dependientes de las acciones que impulse el gobierno federal.

Por lo tanto, se recomienda a México tener en consideración el Convenio de Budapest[348] como un modelo en ciberdelincuencia que permitiría homologar su legislación con la normatividad internacional, por lo que si se ratifica, ayudaría a mejorar sus capacidades legales en cuanto al combate a la delincuencia cibernética, de manera que se podría colaborar y cooperar de una manera más eficiente a nivel regional e internacional.[349]

Respecto al CERT, se hace mención de que se debe establecer un centro de respuesta que tenga un objetivo específico, para que su efectividad sea alta, puesto que si tiene un enfoque amplio, se limita su funcionalidad al atender diversos problemas. En tal sentido, la sugerencia es que:

> El gobierno federal debería considerar la creación de un CSIRT nacional de infraestructura crítica nacional independiente de cualquier… [institución que tenga otras funciones, para que]… [sus facultades]… [sean] exclusivamente… la protección de la infraestructura crítica y de Internet de México.[350]

Lo anterior fueron algunas recomendaciones que emitió la OEA para que México las considerara en la elaboración de su Estrategia Nacional de Ciberseguridad. La implementación de dicha estrategia se llevó a cabo en noviembre del año 2017, por lo que su creación es reciente; sin embargo, el desarrollo del tópico se estudió a lo largo del sexenio de la gestión del ex presidente Peña Nieto.

---

[348] El Convenio de Budapest es un Tratado Internacional que entró en vigor en el año 2004. Establece una terminología especializada sobre delitos informáticos. De tal manera que, busca facilitar la cooperación con otros Estados en dicha materia con el fin de hacer frente a cuestiones como pornografía infantil, derechos de autor, fraude, entre otras. En "¿Qué es el Convenio de Budapest?", *NIC Argentina*, diciembre 2017, acceso el 12 de octubre de 2018 en: http://bit.ly/2kb8yIB

[349] "Recomendaciones para el Desarrollo…", p. 25.

[350] Ibíd., p. 27.

Aunque la mayor parte de los trabajos ha sido más teórico que práctico, el cúmulo de información, ideas y experiencias a través del trabajo en conjunto con diversos países y organizaciones, puede ser aprovechado por México en el desarrollo de una estrategia de ciberseguridad más amplia.

El objetivo general de la ENC es «identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano».[351] Derivado de dicho objetivo, se deprenden 5 estratégicos, que abordan, sociedad y derechos; economía e innovación; instituciones públicas; seguridad pública y seguridad nacional. Por otra parte, en su estructura también se encuentran presentes tres principios rectores, «Perspectiva de derechos humanos; enfoque basado en gestión de riesgos y colaboración multidisciplinaria y de múltiples actores» y ocho ejes transversales[352] que dan como resultado una estrategia amplia. Gráficamente se puede visualizar en el cuadro número 13 de la siguiente página.

Las definiciones de los 5 objetivos estratégicos son:[353]

> Sociedad y derechos: Generar las condiciones para que la población realice sus actividades de manera responsable, libre y confiable en el ciberespacio, con la finalidad de mejorar su calidad de vida mediante el desarrollo digital en un marco de respeto a los derechos humanos como la libertad de expresión, vida privada y protección de datos personales, entre otros.
>
> Economía e innovación: Fortalecer los mecanismos en materia de ciberseguridad para proteger la economía de los diferentes sectores productivos del país y propiciar el desarrollo e innovación tecnológica, así como el impulso de la industria nacional en materia de ciberseguridad, a fin de contribuir al desarrollo económico de individuos, organizaciones privadas, instituciones públicas y sociedad en general.
>
> Instituciones públicas: Proteger la información y los sistemas informáticos de las instituciones públicas del país para el funcionamiento óptimo de éstas y la continuidad en la prestación de servicios y trámites a la población.

[351] "Estrategia Nacional de Ciberseguridad", p. 4

[352] Los ejes son cultura de ciberseguridad; desarrollo de capacidades; coordinación y colaboración; investigación, desarrollo e innovación TIC; estándares y criterios técnicos; infraestructuras críticas; marco jurídico y autorregulación, y medición y seguimiento.

[353] "Estrategia Nacional de Ciberseguridad", p. 18.

Seguridad pública: Incrementar las capacidades para la prevención e investigación de conductas delictivas en el ciberespacio que afectan a las personas y su patrimonio, con la finalidad de mantener el orden y la paz pública.

Seguridad nacional: Desarrollar capacidades para prevenir riesgos y amenazas en el ciberespacio que puedan alterar la independencia, integridad y soberanía nacional, afectando el desarrollo y los intereses nacionales.

CUADRO 13. ESTRUCTURA DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD.[354]

Los cinco objetivos tienen cierta relación con la Estrategia Digital Nacional; no obstante, adquieren un enfoque múltiple en la atención de sectores críticos que deben ser fortalecidos. Parte considerable de la ENC es que tenga un segmento para seguridad nacional, demostrando la coherencia de la política de seguridad multidimensional presentada en el sexenio.

Respecto a los ocho ejes transversales, el gobierno tomó en cuenta algunas observaciones que hizo la OEA en sus recomendaciones, pues incluyeron diversos puntos que se sugirieron en materia de cultura de ciberseguridad, colaboración y coordinación, desarrollo de capacidades, investigación y desarrollo, así como lo referente a normas y estándares técnicos.

[354] Elaboración propia con datos obtenidos de la Estrategia Nacional de Ciberseguridad 2017.

Por otra parte, es necesario destacar que la OEA recomendó que la estrategia fuera implementada por un alto mando de gobierno. En este sentido, la encargada de esta acción en su etapa inicial, es la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE) a través de la Subcomisión de Ciberseguridad. La Subcomisión es supervisada por la Comisión Nacional de Seguridad, que es dependiente de la Secretaría de Gobernación, por lo cual, no está mal, aunque sería ideal establecer una agencia especializada en materia de ciberseguridad para que los trabajos que se desarrollen, tengan un progreso potencial en el corto y mediano plazo.

Las acciones que deberá llevar a cabo la Subcomisión consisten en:[355]

> Aprobar y dar a conocer la Estrategia;
> dar seguimiento y coordinar la implementación de la ENCS en colaboración con las diferentes dependencias y entidades de la APF;
> impulsar los esquemas de colaboración y cooperación interinstitucional en materia de ciberseguridad, y;
> fomentar la colaboración y cooperación con los diferentes actores interesados: sociedad civil, sector privado, comunidades técnicas y académicas.

Algunas recomendaciones adicionales que sugiere la OEA en su documento «Un llamado a la acción para proteger a ciudadanos, sector privado y Gobierno», son la promoción de ciberejercicios sectoriales para mejorar el aspecto operativo ante ciberataques, así como el desarrollo de códigos y buenas prácticas que incentiven una mejora en los estándares de certificación. En el ámbito de la ciberdefensa, se sugiere tomar en cuenta los siguientes puntos:

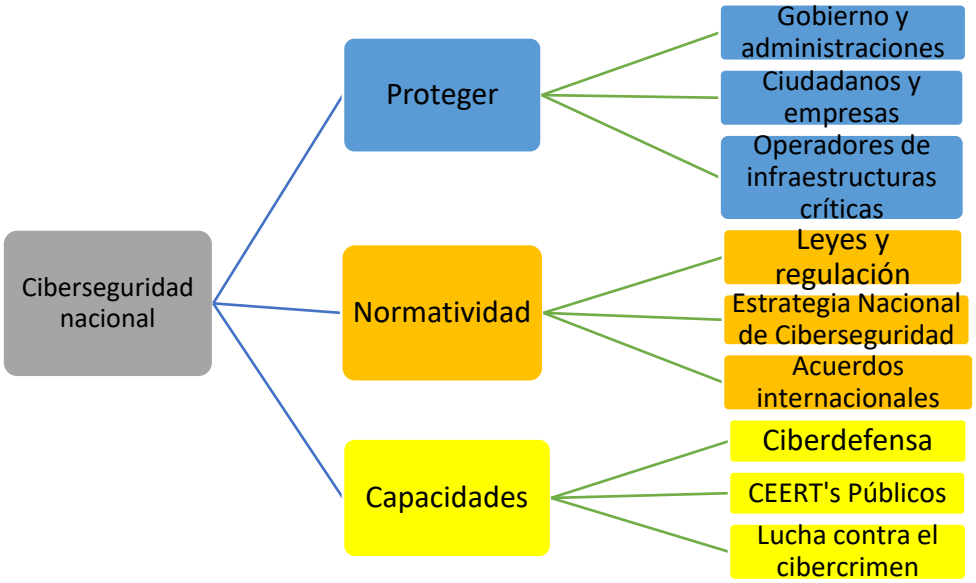
> Desarrollar planes específicos de especialización y entrenamiento en la materia, que permita que los ejércitos cuenten con los efectivos necesarios;
> definir un modelo de colaboración con empresas especializadas y con expertos en ciberseguridad para reforzar las capacidades de las fuerzas armadas en los casos que se determinen;
> promover ciberejercicios periódicos que faciliten el entrenamiento continuo sobre escenarios reales;
> desarrollar conocimiento y experiencia sobre amenazas y vulnerabilidades relacionadas con la ciberdefensa y también métodos de ataque, a través del intercambio de información a nivel nacional e internacional; y

[355] Ibíd., p. 25.

establecer una cooperación con las principales instituciones académicas y de I + D para el desarrollo de necesidades específicas en el ámbito de la ciberdefensa.[356]

Al conjuntar las estrategias y recomendaciones, el modelo de ciberseguridad nacional debe incluir el trinomio de protección, normatividad y capacidades, tal y como se ilustra en el cuadro 14.

CUADRO 14. MODELO DE CIBERSEGURIDAD NACIONAL.[357]



La ENC se elaboró en el año 2017, por lo que su planificación y aplicación es muy reciente. Al estar en una etapa temprana, es prioritario seguir dotándola de los elementos jurídicos y operacionales necesarios para que sea funcional. A su vez, también es un requisito complementar su eje de acción, esto se refiere a que es indispensable el desarrollo de una Ley General de Ciberseguridad, en la que se incluyan los lineamientos jurídicos que den certeza a la Estrategia Nacional de Cibserseguridad. Todo esto no es algo sencillo, puesto que requiere de la negociación en el plano político para poner el tema de la seguridad cibernética como un tópico de urgencia nacional, por lo tanto debe ser tratado en el ámbito ejecutivo, legislativo y judicial.

[356] Miguel Rego, "Un llamado a la acción para proteger a ciudadanos, sector privado y Gobierno", *Organización de los Estados Americanos*, 2018, p. 22, http://bit.ly/2IPQ0hh
[357] Elaboración propia con datos obtenidos del documento "Un llamado a la acción para proteger a ciudadanos, sector privado y Gobierno", Organización de los Estados Americanos (2018).

México debe asumir una posición más comprometida y responsable con respecto al tema de la ciberseguridad, toda vez que uno de sus objetivos consiste en reducir la brecha digital existente en el país, pero para lograr esto deben estar en las mismas condiciones la innovación y los protocolos de seguridad en la información y la red.

En esa tesitura, resulta viable considerar las recomendaciones de la OEA, debido a que esto haría posible incrementar y fortalecer las capacidades de México en los rubros antes descritos, sin embargo es preciso mencionar que no se deben adaptar tal y como lo establece dicha organización, sino que debe ajustarse de acuerdo a las capacidades con las que cuenta México.

Si bien se puede tomar en cuenta lo descrito por la OEA, también es necesario evaluar oportunidades de mejora con otros países, puesto que existen otros Estados con un nivel más desarrollado en el área del ciberespacio y en la relación que existe con la seguridad pública y nacional. En tal sentido, España puede servir como referencia, debido a que desde hace algunos años ha estado trabajando en dicha temática.

En el año 2015, el Consejo Nacional de Ciberseguridad de España, aprobó nueve planes en materia de ciberseguridad, sin embargo, para efectos de esta investigación cito los últimos cinco porque son puntos en los que México puede obtener mejoras graduales. A saber:

- Plan de Protección y resilencia de las TIC en el sector privado;
- plan de impulso al desarrollo industrial, capacitación de los profesionales y refuerzo de la I+D+i[358] en materia de ciberseguridad;
- plan de cultura de ciberseguridad. Concienciación, sensibilización y educación;
- plan de cooperación internacional y UE;
- plan para el intercambio de información sobre ciberamenazas.[359]

Dichos planes podrían ser adaptados en México, puesto que el primero toma en cuenta la resilencia que deben tener las empresas ante eventuales ataques cibernéticos. El segundo parte de la idea de que se debe generar un avance gradual en la profesionalización del personal (servidores públicos) en materia de ciberseguridad, además de impulsar la

[358] La fórmula I+D+i significa Investigación más Desarrollo más innovación.
[359] Ministerio de la Presidencia, "Informe Anual de Seguridad Nacional 2015", *Departamento de Seguridad Nacional*, 2016, España, p. 55, http://bit.ly/2lNVtoQ

investigación para que exista desarrollo y, con ello, innovación. El tercero busca reducir la falta de conocimiento que tienen las personas en el rubro de las tecnologías, en todo caso, la idea central es apostar por construir sociedades de la información y el conocimiento, pero con una perspectiva de seguridad en la información y en las redes. El cuarto tiene una variable que es indispensable para atender los ciberataques, la cual consiste en la cooperación internacional y vincula a la Unión Europea, en este caso, para México, una organización cercana es la OEA y también la región de Norteamérica. Por último establece el intercambio de información, el cual constituye un factor clave para atender los incidentes cibernéticos, en este sentido, entra nuevamente la idea de la cooperación, pero desde la visión de México, el CERT-MX podría servir a este objetivo de trabajo en conjunto con otras divisiones especializadas.

Ante todo esto, es idóneo precisar la siguiente interrogante ¿México tiene la capacidad para mejorar su Estrategia Nacional de Ciberseguridad? La respuesta es que México sí puede hacerlo, pero para ello necesita darle continuidad y destinar presupuesto a los trabajos que realizó la gestión del ex presidente Enrique Peña Nieto. Aún es impreciso saber qué rumbo tomará la administración del actual presidente Andrés Manuel López Obrador 2018-2024 en dicho tema porque no se ha hablado estrictamente sobre el tema en cuestión, sin embargo uno de los tópicos que toma como hoja de ruta, es el tema económico, el cual pretende, a través de las TIC, aumentar la cobertura de *Internet* en diversas zonas del país.[360] Si bien esto es importante, también representa un riesgo debido a que se deben extender a la par campañas de concientización sobre los riesgos en el ciberespacio; es necesario entender que no todas las regiones del país tienen los conocimientos necesarios sobre una navegación segura a través del ciberentorno. Por lo tanto, si se aumenta la conectividad sin una estrategia clara sobre ciberseguridad, es probable que en el corto y mediano plazo emerjan problemas por riesgos cibernéticos. Es por ello que debe existir una relación estrecha entre la ENC y la planeación de aumentar la cobertura de *Internet* en distintas zonas geográficas.

Por lo tanto, dos de los retos para la administración del presidente en turno, Andrés Manuel López Obrador, consisten en, crear un marco jurídico para que la ENC tenga un sustento

[360] "Plan Nacional de Desarrollo 2019-2024", *México Presidencia de la República*, p. 52, acceso el 03 de septiembre de 2019, http://bit.ly/2lPlwMk

legal que obligue a las autoridades a cumplirla, y el segundo tiene como base que se unifiquen los criterios de ciberseguridad en los tres niveles de gobierno.[361]

5.4 La necesidad de la Cooperación Internacional

Con los efectos de la globalización, resulta difícil atender de manera individual los temas que más causan preocupación, tales como el sistema financiero, el comercio, el cambio climático, la migración, el crimen organizado, el terrorismo y también la ciberseguridad.

Tal escenario implica para México tener iniciativas que den sustento a la colaboración y cooperación en materia de ciberseguridad para hacer frente a los efectos derivados de los riesgos en el ciberespacio. En tal sentido, es pertinente hacer énfasis en que las acciones de política exterior del Estado mexicano, casi siempre tienden al multilateralismo, de modo que en la elaboración de los intereses nacionales, se puede proyectar el desarrollo de la ciberseguridad desde un plano meramente de protección y seguridad a nivel bilateral y regional.

Dicho sustento se encuentra tipificado en la Constitución Política de los Estados Unidos Mexicanos. En su artículo 89, fracción X, se especifican las atribuciones del Poder Ejecutivo Federal en materia de Política Exterior, así como los criterios normativos que deben seguirse en el accionar de México a lo largo del tiempo, de tal manera que, los principios son los siguientes:

> La autodeterminación de los pueblos; la no intervención; la solución pacífica de controversias; la proscripción de la amenaza o el uso de la fuerza en las relaciones internacionales; la igualdad jurídica de los Estados; la cooperación internacional para el desarrollo; el respeto, la protección y promoción de los derechos humanos y la lucha por la paz y la seguridad internacionales.[362]

La cooperación internacional para el desarrollo y la lucha por la paz y la seguridad internacionales, se encuentran presentes, lo que da un amplio margen de acción para que México pueda cooperar en materia de incidentes cibernéticos.

Las innovaciones digitales han hecho casi obligatorio que la colaboración sea indispensable para afrontar los riesgos y amenazas que se encuentran en el ciberespacio, pues las

[361] Rodrigo Riquelme, "Marco jurídico, reto del próximo gobierno en ciberseguridad", *El Economista*, 02 de agosto de 2018, acceso el 12 de octubre de 2018 en: http://bit.ly/2keh5uk

[362] "Artículo 89 constitucional", *Orden Jurídico*, acceso el 12 de octubre de 2018 en: http://bit.ly/2m5lBM5

políticas y estrategias elaboradas por un Estado no son suficientes para atender la naturaleza de los nuevos conflictos, especialmente porque que trascienden fronteras y adquieren un dinamismo global rápidamente.

Las actuales condiciones requieren de nuevos mecanismos y estrategias modernas. En tal sentido, Carlini menciona:

> La interdependencia de las redes reclama un enfoque holístico para poder garantizar un nivel satisfactorio de seguridad en el ciberespacio. Razón por la cual los responsables políticos y los expertos creen en la importancia de la cooperación entre naciones, logrando, como objetivo último, la capacidad de prevenir el ataque, enfrentarse mientras está ocurriendo, responder activamente, reducir al máximo posible sus efectos, encontrar su origen y establecer la función original.[363]

De manera similar, Arteaga señala:

> Dentro de la acción exterior de los Estados, se puede tener dos enfoques de la dimensión internacional de la ciberseguridad: uno vertical, en el que cada actor proyecta su actuación hacia el ámbito global, y uno transversal, en el que se integran todos los ámbitos verticales antes de proyectarlos hacia el exterior. Adoptando uno u otro enfoque, los gobiernos pueden elegir entre cada actor público y privado [para que puedan internacionalizar sus intereses de manera individual, o bien, de manera conjunta, a fin de que]… añada valor y economía de escala a su acción exterior.[364]

Dichas aportaciones hacen énfasis en la acción exterior como una forma eventual de atender un problema, desafío u oportunidad. Para el caso de México, los tres se encuentran presentes porque representan un problema las pérdidas económicas por motivo de ciberataques; son un desafío debido a que las políticas y acciones en algunos sectores son insuficientes, y por otra parte, pueden ser una oportunidad si se desarrolla innovación e investigación en el ámbito del ciberespacio y la ciberseguridad. Sin duda, representaría para el país un valor agregado en su economía y su compromiso internacional.

México ha llevado a cabo acciones de cooperación en algunas materias, de acuerdo a los intereses nacionales que se tengan. Un ejemplo práctico de esto fue la elaboración de la

[363] Agnese Carlini, "Ciberseguridad: un nuevo desafío para la comunidad internacional", *Instituto Español de Estudios Estratégicos*, Documento de opinión, 2016, p. 14, http://bit.ly/2m3f7xg

[364] Félix Arteaga, "La dimensión internacional de la ciberseguridad", *Real Instituto Elcano Royal Institute*, 24 de julio de 2018, acceso el 12 de octubre de 2018 en: http://bit.ly/2kFWMWG

Estrategia Nacional de Ciberseguridad, en la cual la OEA brindó asistencia técnica al respecto.

Con base a lo anterior, las instituciones del Estado mexicano han generado grandes aportes en la definición de términos sobre el ciberespacio y sus derivados; por lo que pueden ser considerados por otras naciones en el desarrollo del tema, a nivel regional e internacional. En la sección final de la ENC se encuentra el glosario de conceptos, el cual, si el tema sigue en constante actualización, el tópico puede ser un referente en la región.

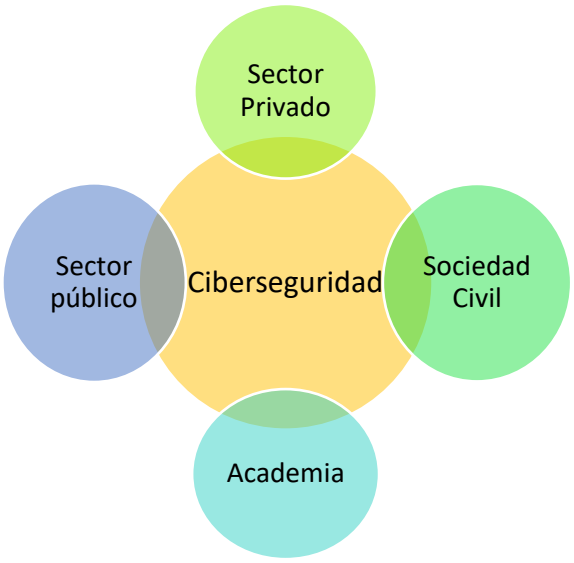
En lo que respecta a las deficiencias, cabe decir que, la falta de preparación cibernética, marcos jurídicos, políticas y estrategias a nivel nacional, hacen vulnerable a México. Aunado a esto, otra dificultad que puede enlistarse consiste en que algunas empresas e instituciones públicas, se muestran reticentes en la disposición de colaborar en la investigación de las amenazas cibernéticas.[365]

Lo anterior dificulta la instrumentación efectiva de un modelo de ciberseguridad nacional que sea sólido y resiliente, pues permite que se generen asimetrías con el crimen organizado, terroristas, Estados y otros grupos delictivos que se ponen a la vanguardia en las innovaciones tecnológicas digitales. Para hacer frente a tal escenario, es un requisito establecer canales de comunicación que permitan fortalecer los instrumentos de inteligencia a través del intercambio de información[366] con entidades nacionales e internacionales.

Si bien algunas instituciones en México han estado trabajando en dicha temática, el principal factor que puedo determinar cómo negativo es que no se le ha otorgado el impulso adecuado para generar una estrategia sólida y que sea operativa en toda la República. De momento, el país está pasando por una etapa de investigación y prueba, puesto que el trabajo más reciente fue la Estrategia Nacional de Ciberseguridad. De manera gradual, puede que México pase a un nivel que sea operativo y propositivo, pero para lograrlo debe invertir más en el mismo teniendo en cuenta las debilidades que posee. En este sentido, se debe integrar la cooperación a través del siguiente cuadrinomio estratégico: sector público, privado, sociedad civil y academia.

[365] Julio Sánchez, "Colaboración y divulgación, desafíos de la ciberseguridad en México", *El Economista*, 17 de agosto de 2017, acceso el 12 de octubre de 2018 en: http://bit.ly/2lL618j
[366] Ibíd.

CUADRO 15. PROMOCIÓN DE LA CIBERSEGURIDAD.[367]



El eje transversal de la ENC, en su apartado «coordinación y colaboración», estipula cuatro acciones que fomentan la cooperación, siendo las siguientes:

> Fortalecer la cooperación y colaboración internacional.
> Identificar los mecanismos de coordinación y cooperación entre los distintos actores involucrados a nivel nacional.
> Definir y aplicar el modelo de gobernanza de ciberseguridad entre sociedad civil, sector privado, academia e instituciones públicas para compartir información y mejores prácticas en materia de ciberseguridad.
> Establecer protocolos y canales de comunicación que fortalezcan la confianza, reciprocidad, y estimulen la responsabilidad social de todos los actores.[368]

Pese a que México ha desarrollado el tema de la ciberseguridad, los trabajos aún son incipientes y falta mucho por hacer, sobre todo en investigación, puesto que dicha área tiende al cambio y la innovación casi permanentes. El estudio de este sexenio es fundamental porque establece las primeras bases en cuanto la definición de una política multidimensional de seguridad en el que incluye al ciberespacio como un factor de riesgo. Además, también ha trabajado, en conjunto con países y organizaciones como la OEA y el Grupo de Expertos Gubernamentales de las Naciones Unidas, en lo que respecta a la seguridad cibernética.

[367] Elaboración propia.
[368] "Estrategia Nacional de Ciberseguridad…", p. 20.

México ha apostado por la digitalización al llevar a cabo la implementación de la Estrategia Digital Nacional, sumándose a los diversos países que están instrumentando los elementos de la Cuarta Revolución Industrial a sus sectores productivos y sociales. Dicho criterio es relevante de enmarcar, pues México podría aportar mucho a nivel bilateral, regional e internacional si se le da continuidad a lo desarrollado en este sexenio en dicha materia. En el marco de la globalización y la CRI, se debe dar dinamismo a la cooperación y colaboración con otros Estados y organismos internacionales que puedan ayudar al país a estar a la vanguardia de los principales retos tecnológicos del siglo XXI.

El tema de la ciberseguridad representa para México retos, pero también oportunidades de desarrollo, de modo que si se toma en cuenta su compromiso a nivel nacional e internacional, se podría volver un referente en seguridad cibernética.

CONCLUSIONES

Para entender la realidad, es necesario crear nuevos enfoques de análisis para identificar los factores de riesgo que pueden producir inestabilidad en el orden público nacional e internacional. En este sentido, la ciberseguridad es un tema que tiene un desarrollo reciente; sin embargo, a raíz del incremento y sofisticación de los incidentes cibernéticos, la preocupación por los asuntos de la seguridad en el marco de la globalización y los efectos de la Cuarta Revolución Industrial, han hecho posible, visualizar lo informático como una herramienta que puede afectar negativamente la seguridad nacional de los países. Por ello, se desarrolló esta investigación denominada: «Cambios en la seguridad internacional en el marco de la globalización: el caso de la ciberseguridad y sus desafíos para la Seguridad Nacional de México (2012-2018)».

Por lo tanto, se planteó al inicio de esta investigación que el sistema internacional se ha configurado de muy diferentes maneras, debido, principalmente, a los efectos que la globalización ha impulsado. Uno de los cambios más significativos se centra en el surgimiento de nuevos actores en el escenario global, los cuales pueden ser entes estatales, o bien, no estatales, como empresas, grupos delictivos o terroristas, entre otros.

Además, el marco de la Cuarta Revolución Industrial ha dinamizado las relaciones entre dichos actores, generando nuevos alcances y espacios que les permiten proyectar sus objetivos e intereses a través del empleo de las Tecnologías de la Información y de la Comunicación. Con base en ello es que surge la necesidad de entender cómo las tecnologías digitales pueden incidir en la seguridad internacional y nacional de los Estados. Ante tal escenario, es indispensable reformar y actualizar la Ley de Seguridad Nacional de México del año 2005, toda vez que requiere ser adaptada de acuerdo a la coyuntura tecnológica-digital.

El ciberespacio es una herramienta estratégica que permite proyectar intereses económicos, políticos, militares, sociales, entre muchos otros que, particularmente, tienden una tendencia a favorecer los mismos a través de la utilización de acciones ofensivas en contra de otros actores.

En esa tesitura, se enfatiza la premisa de que la globalización y la Cuarta Revolución Industrial, han hecho posible que se materialicen nuevos riesgos y amenazas, de modo que,

se destaca el debate existente sobre los estudios de seguridad, el cual ha cobrado más rigor a partir del fin de la Guerra Fría y posteriormente con los atentados terroristas a las Torres Gemelas el 11 de septiembre de 2001 en los Estados Unidos, de modo que la crítica reside en el concepto de la seguridad restringida o tradicional con su contraparte multidimensional, la cual toma como referencia nuevos temas que no sólo hacen énfasis a cuestiones militares.

Surgido de dicho debate se hace énfasis de que el ciberespacio puede y debe categorizarse como un asunto de seguridad nacional y seguridad pública. Para ello, la investigación retomó tres sucesos internacionales, los cuales hacen referencia a lo acaecido en Estonia, Irán con *Stuxnet* y lo que causó *WannaCry*. Por otra parte, se particularizó en la situación de México en dicha materia. Con base en lo anterior, se evidenció que el país sí tiene resultados desfavorables a causa de ataques cibernéticos.

El desarrollo del primer capítulo explicó el marco teórico y conceptual de los términos clave para abordar la investigación. Para ello, el marco de referencia que tomó fue la globalización en el contexto de la Cuarta Revolución Industrial como eje de la expansión tecnológica-digital, debido a que tiene como elementos de desarrollo, el Internet de las Cosas, los sistemas ciberfísicos, la robótica, la nube, entre otros, que tienen como características, la interconexión y el flujo masivo de datos. Las empresas, organizaciones e instituciones gubernamentales tienden a incursionar en tales innovaciones por los beneficios que traen consigo. No obstante, los flujos de información requieren de una mayor capacidad de almacenamiento en procesadores y ordenadores.

Si bien traen beneficios en diferentes sectores, el desarrollo de capacidades cibernéticas también puede ser empleado para realizar acciones ofensivas en contra de otros actores, de modo que el ciberespacio puede ser utilizado para hurtar información, dinero o dañar ordenadores e infraestructuras críticas. De tal manera que, los riesgos y amenazas a la seguridad nacional e internacional, se encuentran a la orden del día por los efectos negativos que pueden causar las innovaciones digitales si se les da un uso incorrecto.

El proceso de la globalización ha transformado la sociedad internacional de distintas maneras, permitiendo la creación de nuevos canales de participación para actores que antes no tenían tanto protagonismo, tales como el crimen organizado, grupos terroristas (*Daesh*), *hackers* como *The Shadow Brokers*, *Anonymous*, e incluso empresas trasnacionales que,

con el poder que han adquirido pueden hacer uso del ciberespacio para robar información respecto a sus contrapartes, es decir, sus competidores. Es en este contexto que los flujos de información en el ciberespacio adquieren un sentido amplio en la navegabilidad del espacio virtual porque no tienen un límite geográfico, permitiendo una mayor interacción entre sociedades y Estados, puesto que las características de velocidad, alcance e intensidad dinamizan dichos intercambios. .

Considerando que las Tecnologías de la Información y la Comunicación (TIC) pueden ser utilizadas para propósitos bélicos, un aumento significativo en las capacidades tecnológicas-digitales por parte de un Estado, fuerza a los demás a caer en el dilema de la seguridad, provocando una competencia directa en el desarrollo de la seguridad y la defensa en el plano virtual, tal es el caso de Estados Unidos de América, el cual invierte grandes cantidades de dinero para mejorar sus capacidades cibernéticas, así como también realiza ejercicios en conjunto con otros países como Japón[369]; en ese tenor, Rusia y China también destinan partes de sus presupuestos para estar a la vanguardia en dicha materia.

Por otra parte, los estudios de seguridad se han ido adaptando a la coyuntura de la sociedad internacional, generando para ello, una serie de debates y análisis que permiten visualizar nuevos riesgos y amenazas que antes no se consideraban, pero que ahora, con el proceso de globalización, son tomados en cuenta por los daños que pueden llegar tener de manera general y particular. En ese tenor, se establece una crítica al carácter restringido tradicional de la seguridad por no poder brindar soluciones a problemas de naturaleza diversa a través de acciones bélicas.

Con base en ello, la seguridad nacional de todo Estado debe atender los intereses nacionales, de modo que necesitan ser proyectados para lograr un pleno desarrollo. Para que esto suceda, se tienen que establecer cuáles son los intereses nacionales en materia de seguridad nacional en el corto, mediano y largo plazo. Además, se requiere tener de las capacidades materiales e inmateriales (capital humano) que hagan posible crear una política de seguridad multidimensional para hacer frente a los riesgos, amenazas y desafíos tecnológicos del siglo XXI.

[369] Infosecurity, "Japón desarrollará una agencia de élite de sombreros blancos", *UNAM-CERT*, 20 de mayo de 2016, acceso el 20 de junio de 2019 en http://bit.ly/2kDmkDZ

A su vez, la Teoría de Complejos de Seguridad Regional permite partir de un objeto referente, que en el ámbito de la seguridad, precisa un análisis particular de algún asunto, en este caso, el de la ciberseguridad. De este modo, se utilizó esta teoría para explicar cómo el aspecto securitizador puede expandir la agenda de seguridad de un Estado si un asunto es considerado crítico. Por tal motivo, se argumentó que los ciberataques son utilizados para favorecer múltiples intereses, entre los que destacan cuestiones industriales, comerciales, políticas, militares, diplomáticas y sociales, por lo que se debe tomar la seguridad cibernética como un tema emergente para su desarrollo, esto si se tiene en cuenta el progreso que han tenido otros actores en el ámbito regional e internacional sobre dicha materia. Al considerar lo anterior, es posible formar un sustento que dé pie al proceso securitizador.

El Estado es el garante de la seguridad, por lo que debe generar un entorno adecuado en el ciberespacio para todos aquellos individuos, empresas, organizaciones y demás sectores que utilizan la interconexión para sus operaciones diarias. También es prioritario salvaguardar la información de las instituciones gubernamentales a través de la elaboración de controles de riesgo e implementación de políticas de seguridad integrales en las que se tome en cuenta la ciberseguridad y la seguridad de la información. Con los avances tecnológicos digitales, los riesgos cibernéticos adquieren mayor intensidad debido a que los factores y motivaciones de los atacantes son múltiples. Los que emplean el ciberespacio para llevar a cabo acciones ilícitas, aprovechan las características del ciberespacio (bajo costo, fácil ejecución, efectividad, impacto y anonimato).

La presente investigación retomó los trabajos que han realizado las organizaciones internacionales en el ámbito de la ciberseguridad, tales como la Organización de las Naciones Unidas, la Unión Internacional de Telecomunicaciones, la Organización del Tratado del Atlántico Norte, la Organización de los Estados Americanos y en el ámbito regional la Unión Europea.

La ONU, que tiene por objetivo, velar por el mantenimiento de la paz y seguridad internacionales, ha realizado estudios que fundamentan la preocupación sobre el asunto de la seguridad cibernética. En la resolución 53/70, la UNODA abordó el tópico en cuestión y concluyó que existen diversas problemáticas que pueden generar inestabilidad en la seguridad internacional, especialmente, en materia de la información y de las

telecomunicaciones. Aunado a esto, también ha presentado diversos informes, siendo éstos los siguientes: «A/65/154, A/66/152, A/67/167, A/68/156, A/69/112, A/70/172».

En dichos informes, el Grupo de Expertos Gubernamentales (GEG) ha expuesto que la cooperación bilateral, regional e internacional son vitales para hacer frente a los desafíos que representan el cuidado de la información y las telecomunicaciones. En ese sentido, México puede optar por suscribir acuerdos de cooperación con Estados Unidos, Canadá u otros países de manera bilateral o regional, aunque por cercanía geográfica y acuerdo comercial, su región más próxima es América del Norte.

En los estudios realizados por el GEG, se estipulan los principales riesgos, entre los que destacan: ataques a infraestructura crítica y bloqueo a sistemas digitales. Ante tal coyuntura, destacó que los Estados y el terrorismo representan amenazas reales, debido a que, de manera gradual, aumentan sus capacidades cibernéticas con fines bélicos, lo que puede causar posibles conflictos entre los mismos. Esto refuerza el concepto del dilema de la seguridad y da certeza de que el empleo de la tecnología con fines ilícitos, puede causar inestabilidad en la seguridad nacional e internacional por tales factores.

Parte relevante del trabajo de la ONU reside en que la discusión es planteada en el marco de la Asamblea General, esto permite conocer los avances y estudios realizados por el Grupo de Expertos Gubernamentales con el propósito de que los Estados miembros puedan dimensionar el tópico de la ciberseguridad, y con ello, contribuyan dando a conocer su desarrollo, además de expresar oportunidades de mejora en la materia.

La UIT es otro organismo especializado de la ONU en el ámbito de las TIC. Parte relevante de su trabajo es el desarrollo del Índice Mundial de Ciberseguridad que, a través de sus parámetros, mide el nivel de los países al respecto. Por otra parte, el trabajo de los integrantes sirve como punto de enlace entre el sector público y privado de diferentes países.

En el ámbito regional, la Unión Europea ha fortalecido la seguridad cibernética desde la creación de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, por sus siglas en inglés) en el año 2004, por lo que ha generado grandes avances en los países que la conforman, pues la aplicabilidad de sus leyes y reformas es general. En ese sentido, el desarrollo del ciberespacio reside en el fortalecimiento del sector económico, debido a que es un sector estratégico en la era de la informatización y digitalización que permite mayores

avances en la productividad. Sus estrategias y políticas son integrales, pues el propósito es crear una economía digital competitiva. Los trabajos de ENISA, la Agenda Digital y la aplicabilidad de la Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión, mejor conocida como Directiva NIS, implican para la Unión Europea, robustecer sus estándares en materia cibernética, de modo que todos los Estados que la conforman deben cumplir con niveles óptimos en ciberseguridad.

En una línea similar, la OTAN y su relevancia estratégica en lo político-militar, tiene su sustento en los artículos 5 y 6 de su carta constitutiva en la que priorizan la defensa colectiva de los Estados miembros. En ese sentido, han procurado adaptarlos a las circunstancias virtuales del ciberespacio, creando para ello, divisiones y comités especializados. Tal es el caso del Centro de Excelencia de Defensa Cibernética Cooperativa, el cual desarrolla distintas investigaciones y elabora rigurosos estudios en materia de ciberseguridad y ciberdefensa.

Además, con la Cumbre de Lisboa del año 2010, se aprobó el Nuevo Concepto Estratégico, dando a conocer que los ciberataques son un reto global porque cada vez se incrementan y adquieren mayor protagonismo por parte de Estados y otros actores no estatales. A su vez, en el año 2011, entró en vigor su Nueva Política de Ciberdefensa, en la que otorgaron la facultad al Consejo del Atlántico Norte para deliberar en qué momento un ciberataque puede ser considerado un asunto de defensa colectiva. En tal sentido y considerando lo crítico que puede ser invocar el artículo 5 de su carta constitutiva, se dotó al Consejo de dicha facultad para que evalúe en qué momento se puede actuar bajo el principio de defensa colectiva, toda vez que las características en el ciberespacio hacen difícil saber con exactitud dónde ocurre un ataque cibernético y quién lo lleva a cabo. La Cumbre de Varsovia del año 2016 complementó lo anterior, porque calificaron como nuevo dominio de operaciones al ciberespacio, y con esto, lograron ampliar su ámbito de acción en el desarrollo de ese rubro.

La Organización del Tratado del Atlántico Norte es un gran referente en el ámbito de la seguridad y defensa, el que haya calificado como nuevo dominio de operaciones al espacio cibernético tiene dos significados, el primero consiste en que las amenazas son reales, de modo que representa un peligro para la organización y para los Estados que la conforman.

El segundo se refiere a que los miembros deben adaptar y destinar presupuesto hacia dicho tópico para evitar ser un país con bajos niveles en materia de ciberseguridad y defensa.

La Organización de los Estados Americanos (OEA) adquiere un protagonismo importante para el continente hemisférico al considerar la naturaleza y magnitud que pueden tener las amenazas y riesgos desde un enfoque multidimensional, siendo su base, la Declaración sobre Seguridad de las Américas del año 2003. Desde dicho año, la organización comenzó a elaborar estudios sobre seguridad cibernética, lo que permitió profundizar en la temática para ayudar a los Estados miembros en el desarrollo de estrategias y políticas, para el mantenimiento de la paz y seguridad en el Hemisferio. En tal sentido, también existen las Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA), el cual puede aprovechar México para mejorar su situación en materia de delito cibernético a través de cooperación técnica en materia jurídica.

En otro sentido, la presente investigación también abordó el rol que tiene la innovación tecnológica como punto clave de los efectos bélicos. La implementación de nuevas estrategias ofensivas y defensivas, hace posible la adaptación y evolución de los propósitos de guerra, tal como sucede en el contexto de la Revolución de los Asuntos Militares. Actualmente, la tecnología permite infringir más daño a un adversario, pues la variable de un mayor número de soldados, puede ser sustituida por un arma más sofisticada y con costos más bajos en el espacio virtual, de modo que sólo es necesario tener un ordenador, sistema y los conocimientos en informática, para crear códigos que cumplan con el rol de dañar y destruir infraestructuras vitales. Esto puede hacerlo una persona, pero si son más, es decir, un grupo de personas con conocimientos especializados, pueden crear, desde cualquier parte del mundo, una o más armas cibernéticas que tengan como propósito hacer inoperable el correcto funcionamiento de un dispositivo electrónico.

De manera similar a la OTAN, Estados como Francia, Alemania, Finlandia y los Países Bajos han declarado al ciberespacio como un dominio de guerra. Por lo tanto, es normal esperar que comiencen a crear armamento cibernético que tenga como propósito realizar acciones ofensivas y defensivas en dicho espacio virtual. En ese tenor, en el año 2011, el Departamento de Defensa de los Estados Unidos destinó $500 millones de dólares para el

desarrollo de tecnologías en el ámbito del ciberespacio.[370] Por lo tanto, se puede inferir que el propósito de los Estados y actores no estatales, consiste en crear capacidades para generar ciberpoder.

Ante tal escenario, es posible caer en el dilema de la seguridad, debido a que, si ciertos Estados logran consolidar un fuerte ciberpoder, en consecuencia, otros Estados estarían obligados a desarrollar capacidades cibernéticas para disuadir al adversario. Esto generaría controversias a nivel internacional y ampliaría el conflicto hacia un escenario en el que otros Estados se verían obligados a participar. Además, se intensificarían los problemas, esto si se tiene en cuenta que la mayor parte de los ciberataques cumplen con diversas características, sin embargo, las más controversiales son el anonimato y la rapidez con la que se desarrolla un ataque cibernético.

El 26 de abril del año 2007, Estonia fue víctima de ciberataques de tipo Denegación de Servicio, que tenían como objetivo sobrecargar las páginas *web* de instituciones estratégicas. Tal escenario ocasionó que ciertas actividades se paralizaran en el sector financiero y de gobierno, puesto que el ataque antes mencionado tiene por objetivo sobrecargar de información un sitio en *Internet.* Por lo tanto, las personas no pudieron acceder a las plataformas de sus bancos para realizar operaciones financieras, y de forma similar, también pasó lo mismo con páginas oficiales del gobierno.

En 2010, se llevó cabo el ataque *Stuxnet* contra las centrifugadoras de Irán, que tenían como función el proceso de enriquecimiento de uranio. El gusano informático aprovechó las vulnerabilidades *Zero-day* y alteró las velocidades de rotación establecidas en el código original. Los daños son considerables porque perjudicó aproximadamente 1,000 máquinas, haciéndolas inservibles. Esto ocasionó que Irán mermara dicho proceso, situación que presenta dos variables que son necesarias destacar: la primera consiste en que Irán tuvo que solucionar el problema que ocasionó dicho virus, debido a que tuvo pérdidas económicas al detener el trabajo de las centrifugadoras. La segunda reside en que Irán se vio forzado a mejorar sus capacidades en seguridad cibernética.

El otro suceso que tuvo un impacto considerable fue *WannaCry*, que en el 2017, ocasionó estragos globales en aproximadamente 150 países, dañando a empresas, instituciones e

[370] "El nuevo campo de entrenamiento…".

individuos. El efecto directo se vio reflejado en los costos económicos que causó el virus *ransomware*, puesto que la especialidad del mismo, consistió en cifrar archivos que se encontraban en los ordenadores. El peligro de dicho virus fue la velocidad con la que se expandió a nivel global, evidenciando que las características del ciberespacio se encuentran presentes, particularmente el anonimato y la velocidad.

Parte importante de su propagación se refiere al hecho de que se utilizó *Eternal Blue*, una herramienta robada a la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés*)* de los Estados Unidos por acciones del grupo de *hackers* denominado, *The Shadow Brokers*, demostrando la participación indirecta de una entidad gubernamental en el desarrollo de códigos sofisticados para causar daños desde lo informático. Esto demuestra dos elementos clave en materia de cibertaques y ciberseguridad. El primero tiene que ver con que la Agencia de Seguridad Nacional de Estados Unidos fue vulnerada, esto permite dimensionar que a pesar de tener las mejores condiciones en seguridad cibernética, cualquiera puede ser víctima de un ciberataque. Lo segundo consiste en que se pudo observar lo crítica que puede llegar a ser una arma cibernética al utilizar códigos especializados.

Los ciberataques son considerados por el Foro Económico Mundial, en su informe «*Global Risk Report*», como uno de los cinco problemas con mayor probabilidad de materializarse en el corto, mediano y largo plazo, por lo que son un riesgo latente para los Estados más desarrollados y para los que se encuentran adaptando las tecnologías digitales a sus sectores productivos y de gestión institucional. En ese sentido, el caso de estudio fue México.

En territorio mexicano existen aproximadamente 65 millones de personas que navegan en el ciberespacio, lo que representa un 59 por ciento de los habitantes en el país. Aunado a ello, cabe puntualizar que, la mayoría de la población no tiene los conocimientos necesarios sobre cuestiones cibernéticas, lo que permea en el desarrollo de diversos sectores, pues esto sirve de estímulo para que el cibercrimen siga creciendo. Basta saber que al sector financiero de México le cuesta 107 millones de dólares anuales luchar contra el cibercrimen.[371] Además, de acuerdo con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), en 2015, realizó una estimación de

[371] Gabriela Chávez, "El cibercrimen le cuesta 107 mdd a la banca mexicana: OEA", *Expansión*, 11 de julio de 2019, acceso el 12 de julio de 2019 en: http://bit.ly/2kE7X2g

que las personas pierden alrededor de 150 millones de pesos por ataques cibernéticos al utilizar servicios financieros.[372] Esto supone que a México le falta invertir más para mejorar no sólo su capacidad en seguridad cibernética, sino que debe incentivar también un mercado laboral con gente capacitada en dicha materia.

El grupo *The Shadow Brokers*, reveló que la *NSA* llevó a cabo acciones de ciberespionaje en contra de la SEGOB, SEDESOL y la UNAM, lo que es preocupante, puesto que son instituciones estratégicas para la nación. Además, las estadísticas de *SonicWall* elaboradas en el año 2018, precisaron que México fue el tercer país con mayor índice de ataques a nivel mundial, los otros dos países son Reino Unido de la Gran Bretaña e Irlanda del Norte y los Estados Unidos de América.[373] En ese tenor, basta establecer la siguiente premisa, si los dos países antes mencionados sufren de ciberataques y son considerados Estados con una capacidad fuerte en innovación tecnológica, ¿qué le puede esperar a México? La respuesta no es sencilla, pero es prioritario mencionar que si México quiere aumentar su cobertura digital y proveer de acceso a *Internet* y Tecnologías de la Información y la Comunicación a diferentes segmentos de la sociedad civil, entonces también debe fortalecer sus capacidades en ciberseguridad.

Al considerar el rol de las instituciones estratégicas en el ámbito de la seguridad y defensa, tenemos que la Policía Federal cuenta con el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX), creado en el 2010, el cual se encarga de vigilar y salvaguardar la infraestructura crítica del país. Aunado a ello, tiene divisiones especializadas para atender las cuestiones del ciberespacio; no obstante, se puntualizó que, si se incrementa la carga de trabajo al CERT-MX, posiblemente se podría reducir su efectividad en la atención de los incidentes cibernéticos. Si bien existe cooperación interinstitucional, no todas las instituciones y dependencias tienen altos estándares en ciberseguridad, lo que dificulta que haya un trato oportuno y eficaz de los incidentes cibernéticos, es por esto que es una necesidad urgente incrementar los niveles de ciberseguridad en el ámbito legislativo y judicial, pero también a nivel estatal y municipal.

[372] Carmen Álvarez, "México más vulnerable…"
[373] Omar Ortega, "México, la tercera nación con…"

El Centro de Investigación y Seguridad Nacional (CISEN) tiene como propósito la generación de inteligencia estratégica para que las instituciones encargadas de la defensa y seguridad puedan tomar acciones respecto a los riesgos y amenazas, tal y como se plasma en la elaboración de la Agenda Nacional de Riesgos, en lo referente a los factores que pueden causar inestabilidad en el país. La importancia de esta institución radica en su contribución a los estudios de seguridad nacional y definición de riesgos y amenazas, puesto que es fundamental partir de una base para determinar cuáles son los antagonismos a los que México debe hacer frente. Además, en la Ley de Seguridad Nacional del año 2005, éste Centro es la figura clave de dicha ley.

La SEDENA y la SEMAR se encargan de la defensa del Estado mexicano. De acuerdo a sus leyes orgánicas, se precisan las principales acciones de dichas instituciones armadas. Es relevante mencionar que estas secretarías acotan el tema de la ciberseguridad y la ciberdefensa de manera separada, es decir que cada una desarrolla sus sistemas en dicha materia. Quizá esto representa una ventaja y desventaja, puesto que cada una responsable de cuidar sus sistemas informáticos y de crear innovaciones tecnológicas en el ámbito militar. En tal sentido la desventaja consiste en que no existe una coordinación directa entre tales instituciones armadas.

Es por ello que el rol de dichas instituciones se considera estratégico para el tema en cuestión, puesto que la Policía Federal a través del CERT-MX, es el primer escudo que tiene México para hacer frente a los ciberataques, además de que puede realizar acciones de cooperación en cuestiones técnicas y de intercambio de información con otras instituciones homologas. El CISEN puede contribuir a perfilar posibles riesgos y amenazas para que las demás instituciones las tengan en cuenta y con ello lleven acciones de prevención.

Las acciones desarrolladas en el sexenio estudiado consistieron en fortalecer las capacidades de ciberseguridad y ciberdefensa debido a que se reconoció al ciberespacio como el cuarto dominio de operaciones, debido a ello, los programas sectoriales tienen objetivos y líneas acción ambiciosos que deben seguir desarrollándose en el corto y mediano plazo.

Respecto a la labor formativa, la UNAM tiene un rol clave, pues su carácter académico le permite contribuir al desarrollo de capital humano especializado en materia de seguridad

cibernética. Además, puede fortalecer la cultura en ciberseguridad en los rubros antermente mencionados para atenuar las deficiencias que actualmente padece México.

En lo que se refiere a las infraestructuras críticas, el Programa para la Seguridad Nacional 2014-2018 específica que el país tiene aproximadamente tres mil instalaciones estratégicas, siendo Petróleos Mexicanos (47%), Comisión Nacional del Agua (17%) y la Comisión Federal de Electricidad (13%) los que figuran con mayor porcentaje en sus estimaciones.[374] En tal sentido es prioritario participar en ciberejercicios con otros países, puesto que es un requisito indispensable mejorar en las capacidades de repuesta ante incidentes cibernéticos, particularmente los que tiene que ver con las infraestructuras críticas del país.

A su vez, el desarrollo de ésta investigación mostró que el sistema financiero de México es un objetivo clave para los ciberdelincuentes por el gran dinamismo de la economía. En ese sentido, el Banco de México ha desarrollado una infraestructura robusta para proteger las transacciones financieras y también ha mejorado sus estándares de seguridad cibernética en su organización interna por las actividades que lleva a cabo. Por lo tanto, en el año 2018, creó la Dirección de Ciberseguridad para mejorar la gestión y la prevención de los delitos cibernéticos, particularmente los que tienen por objetivo los sistemas de pago como el Sistema de Pagos Electrónicos Interbancarios (SPEI).

En el mismo año, se aprobó la Ley *Fintech* en México, siendo necesaria para regular e instrumentar nuevas políticas que salvaguarden la información y las transacciones en el entorno digital bajo el marco *fintech*.[375] Para ello, la Secretaría de Hacienda y Crédito Público y la Comisión Nacional Bancaria y de Valores también contribuyen desde sus competencias, al fortalecimiento del sistema financiero mexicano en el ámbito digital.

En el último capítulo se mostraron los desafíos que tiene México en ciberseguridad en relación con la Seguridad Nacional del país. De este modo, se mencionaron los principales problemas que existen con la Ley de Seguridad Nacional del año 2005 respecto a los

[374] Revisar página 110 de esta investigación.

[375] De lo más relevante que debemos considerar en dicho marco tecnológico financiero son los medios de pago y transferencias, infraestructura para servicios financieros, las criptomonedas, entre otras. Para saber más véase la página 114 de esta investigación.

cambios globales, regionales y locales; especialmente los que se refieren a las innovaciones tecnológicas.

También se destacó el problema que ocasiona no tener una Política de Estado en dicha materia. En este sentido, la mayor parte de los modelos de seguridad en México, se crean a partir de la gestión de administraciones sexenales, perjudicando la consolidación de un sistema coherente a mediano y largo plazo.

Además, con base a las críticas que han realizado diversos expertos, tales como Leonardo Curzio, Jesus De Miguel, Raúl Benítez Manaut, Emilio Vizarretea Rosales, entre otros, se reafirma que es necesario actualizar la Ley de Seguridad Nacional del año 2005, con el propósito de re conceptualizar la Seguridad Nacional de México para que se modernice y esté acorde a los desafíos tecnológicos del siglo XXI. De tal manera, se sugiere reformar la ley para integrar al ciberespacio como un riesgo más en la Ley de Seguridad Nacional para que sirva como base en la creación de nuevas políticas y estrategias, a fin de que sean integrales.

Por otra parte, el Programa para la Seguridad Nacional 2014-2018, se desarrolló desde una perspectiva multidimensional de la seguridad, por lo que tomó en cuenta al ciberespacio como un riesgo y una amenaza que puede alterar la seguridad nacional del país. En ese tenor, los Informes de Gobierno destacaron las actividades realizadas para preservar la seguridad nacional desde el ámbito de la ciberseguridad. De modo que, se logró identificar las acciones desarrolladas por parte de la SEDENA, la SEMAR, la PGR y Policía Federal a nivel nacional e internacional, entre las que destacan: la creación del Protocolo de Colaboración para el Intercambio de Información Relacionada con la Ciberdefensa, Ciberseguridad y Seguridad de la Información en el Ciberespacio entre la Secretaría de la Defensa Nacional y la Secretaría de Marina; así como el establecimiento del Centro de Operaciones del Ciberespacio por parte de la SEDENA, y en lo que respecta a la SEMAR, la creación de la Unidad de Ciberseguridad.

La Estrategia Nacional de Ciberseguridad tiene como precedente la Estrategia Nacional de Seguridad de la Información del 2012, y la base de su instrumentación radica en la necesidad de complementar la Estrategia Digital Nacional impulsada en este sexenio, pues para llevar a cabo la transición a la era digital, se requiere de políticas de seguridad cibernética. La

estrategia abarca el sector social, económico, institucional y de seguridad (pública y nacional).

El seguimiento de la estrategia lo lleva a cabo (en su etapa inicial) la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE), a través de la Subcomisión de Ciberseguridad, que fue supervisada por la Comisión Nacional de Seguridad; sin embargo, como mencionó la OEA en sus recomendaciones, sería pertinente que la Estrategia fuera implementada por una institución de alto nivel desde el inicio. En ese tenor, es preciso que la CIDGE siga dándole el impulso necesario para que en la mayor parte de las secretarías se tengan los estándares básicos en materia de seguridad de la información y seguridad cibernética, debido a que, es importante salvaguardar la información gubernamental, particularmente la que tiene carácter restringido o confidencial. También es indispensable que, en la aplicación de la estrategia se busque integrar al sector privado y a la sociedad civil para que tenga más amplitud y se extienda en todos los niveles y sectores del país, puesto que una de las debilidades existentes consiste en que la ciberseguridad sólo es aplicada de manera individual, es decir, cada quién la adapta de acuerdo a los conocimientos que tiene. Por tal motivo, algunos grupos son vulnerables, tales como la sociedad civil, pequeñas y medianas empresas.

La cooperación internacional es fundamental para México, pues uno de los principios rectores expresados en su política exterior, consiste en realizar acciones de colaboración con organizaciones internacionales y otros Estados. De esta manera, el trabajo en conjunto con naciones más avanzadas en materia de ciberseguridad, le daría a México la posibilidad de adquirir experiencias e intercambiar información para fortalecer los trabajos desarrollados hasta el momento.

Derivado de todo lo anterior, la hipótesis general de este trabajo se comprueba, debido a que el asunto de la ciberseguridad es un tema que se está discutiendo cada vez más en los organismos internacionales y regionales; además, se encuentra en las agendas de políticas públicas de países industrializados y de economías emergentes tales como Estados Unidos de América, Francia, España, Alemania, Estonia, entre otros. La seguridad internacional se encuentra en constante cambio, y por tal razón, los países, organizaciones y otros actores han ido adaptando sus estrategias y políticas de acuerdo a la coyuntura. Tal es el caso de la Unión Europea y la OTAN que han incorporado al ciberespacio de acuerdo a sus intereses.

El caso de la Unión Europea y de la Organización del Tratado del Atlántico Norte presentan diferentes aristas, la primera tiene un enfoque económico, porque instrumenta medidas de seguridad cibernética que son aplicables a todos los países miembros que la conforman, pues el objetivo consiste en impulsar su estrategia digital con fines financieros y comerciales. En lo que respecta a la segunda, el enfoque está orientado a la seguridad colectiva del ciberespacio, por lo que se desarrollan ejes de acción no sólo en ciberseguridad, sino también en ciberdefensa.

Ambos casos pueden ser referentes para México, debido a que tienen un alto grado de desarrollo en el tema. En ese sentido, se pueden crear mecanismos de cooperación para intercambiar información y conocimientos, así como también se pueden establecer ciberejercicios en conjunto que doten a México de mayores capacidades en dichas áreas. Asimismo, se debe buscar aprender más sobre cuestiones jurídicas aplicables en el ciberespacio, toda vez que los delitos informáticos requieren de normas en el mismo sentido.

Los riesgos y amenazas en el ciberespacio son reales y pueden ocasionar daños físicos, tal y como se pudo observar con los sucesos en Estonia, los daños ocasionados por *Stuxnet* en las centrifugadoras de Irán, y con *WannaCry*, el consecuente impacto global que tuvo en distintos países.

México tiene un rezago en materia jurídica, política, de seguridad y defensa, toda vez que su Ley de Seguridad Nacional se estableció en el año 2005, demostrando que está desactualizada y no cumple con los fundamentos de seguridad requeridos para el contexto de la Cuarta Revolución Industrial, especialmente en materia de innovación tecnológica digital. Ciertamente el país tiene diversas vulnerabilidades que representan un riesgo en materia económica, política, de seguridad pública y nacional. Por lo tanto, es correcta la hipótesis de que México tiene que visualizar la ciberseguridad como un factor de desarrollo permanente debido a que la innovación tecnológica se encuentra en constante cambio y ésta es aprovechada por distintos actores de manera global.

En el sexenio de Peña Nieto, México adoptó una política multidimensional de la seguridad en la que, a través de su Programa para la Seguridad Nacional 2014-2018, consideró al ciberespacio como un riesgo para la seguridad nacional. No obstante, como se expuso en esta investigación, hay sectores, tales como el financiero (que ha comenzado a realizar

acciones para atenuar los incidentes cibernéticos), industrial, político y social en los que México tiene vulnerabilidades, lo que ha traído consigo grandes costos económicos, pues las estrategias que se han implementado son relativamente nuevas para el país. En ese tenor, la Estrategia Nacional de Ciberseguridad se creó en el penúltimo año de esta administración, por lo que aún falta robustecerla y aplicarla en el corto, mediano y largo plazo.

Como primera etapa, es importante instruir a personal que labore en toda la Administración Pública Federal, toda vez que ellos tratan información de carácter sensible y confidencial; asimismo, también es indispensable trabajar de manera conjunta con el sector privado, la academia y la sociedad civil para cerrar brechas en cuanto conocimientos sobre los riesgos en el ciberespacio.

Dicho esto, las estrategias no han sido integrales debido a que hay sectores que se han fortalecido, tal es el caso del sector financiero, el cual ha implementado políticas específicamente para atender las necesidades que se requieren. Sin embargo, existen otras áreas en las que no se han realizado creado líneas de acción para atender la problemática en cuestión, ya sea por asuntos de presupuesto, por desconocimiento, o bien, porque no se encuentra en la agenda pública.

México es uno de los países que más recibe ataques cibernéticos. De acuerdo con *Symantec*, 1.5 millones de correos electrónicos son maliciciosos,[376] lo que hace posible que el impacto sea considerable si se tiene en cuenta que existen personas, empresas y entidades gubernamentales que tienen un pleno desconocimiento sobre cuestiones básicas de seguridad cibernética; ante tal escenario, es posible que un virus electrónico pueda cumplir su objetivo, puesto que las condiciones actuales lo hacen posible.

En este caso, es preciso destacar lo ocurrido en Estonia, pues demostró cómo un país puede ser paralizado por ciberataques, en caso de no contar con leyes y estrategias en materia de ciberseguridad. Para México, el no contar con una estrategia integral en dicha materia, puede poner en riesgo la seguridad nacional del Estado mexicano debido a que gran parte de la información y las infraestructuras, tienen componentes electrónicos-digitales.

[376] Rodrigo Riquelme, "Ataques cibernéticos a la cadena de suministro aumentan 78% en un año", *El Economista*, 04 de marzo de 2019, acceso el 29 de junio de 2019, http://bit.ly/2m8GciF

En la era de la informatización y la digitalización, es necesario integrar al ciberespacio como un factor de riesgo para la seguridad nacional, debido a que con el avance de la tecnología y la programación, es posible crear códigos especializados que tengan como propósito hurtar información, dañar equipos, paralizar actividades industriales y destruir infraestructuras críticas.

En ese sentido, México debería considerar lo siguiente:

- Ratificar el Convenio de Budapest del año 2004;
- fomentar el desarrollo académico para formar especialistas en informática y tecnologías digitales;
- establecer un marco educativo general en las instituciones académicas, con el fin de brindar conocimientos para concientizar a la población de los riesgos cibernéticos, y con ello, prevenir la propagación de incidentes informáticos;
- actualizar la Ley de Seguridad Nacional del año 2005, con el fin de adaptarla a la coyuntura actual, para que se encuentre a la vanguardia de las tecnologías de disrupción digital, y sirva de soporte para la instrumentación de nuevas políticas y estrategias al respecto;
- seguir aplicando y modificando el Manual Administrativo de Aplicación General en materia de Tecnologías de Información, Comunicaciones y Seguridad de la Información (MAAGTICSI);
- crear una Ley General de Ciberseguridad con el fin de homologar los estándares en los estados y municipios, así como en los tres poderes de la República Mexicana;
- impulsar la innovación e investigación para la creación de tecnología propia, con el fin de reducir la dependencia actual de productos extranjeros, y;
- fomentar el desarrollo de un mercado laboral competitivo en seguridad cibernética.

A México le falta ser más dinámico en la planificación y edificación de la ciberseguridad en relación con la seguridad nacional. No obstante, se está trabajando el asunto en las instituciones defensivas del país, pero falta integrar a demás entidades que también componen la Seguridad Nacional de México, puesto que en un plano globalizado y de seguridad multidimensional, existen otros actores que también dan certeza a la misma.

Los ataques cibernéticos cada vez son más sofisticados, de modo que en el mediano y largo plazo, tienen mayor probabilidad de materializarse con más frecuencia. Sin duda, México debe prepararse para atenuar los eventuales riesgos y amenazas en el ciberespacio, pues estos son cambiantes y dinámicos. El camino es sinuoso, pero hay muchas oportunidades para México si los tomadores de decisiones alcanzan el objetivo de instrumentar estrategias, políticas y leyes integrales que fortalezcan la ciberseguridad en relación con la Seguridad Nacional.

Por último, México puede ser un referente en la región latinoamericana si logra volverse un líder en dicha materia, y también si consigue proyectar su interés nacional a través de su política exterior en el ámbito regional e internacional.

ANEXO

Respuesta de México sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional.[377]

Evaluación de los problemas de la seguridad de la información	Medidas adoptadas para fortalecer la seguridad de la información	Medidas que se podrían adoptar a nivel internacional para fortalecer la seguridad de la información
Las instituciones bancarias y financieras, así como las dependencias del gobierno federal que atienden temas de seguridad pública y seguridad nacional son las organizaciones en el país que realizan mayores esfuerzos en materia de seguridad informática. Se tiene una Unidad de Delitos Cibernéticos y una Policía Cibernética dentro de la Secretaría de Seguridad Pública Federal para entender ciberdelitos de seguridad pública. Por otro lado, aunque existen esfuerzos aislados para el combate de los delitos cibernéticos en los tres órdenes de gobierno, no existe una política de seguridad cibernética del gobierno federal que guíe las estrategias del combate al cibercrimen en el país, la legislación en la materia requiere ser fortalecida, los jueces requieren contar con más instrumentos que les permitan atender y sancionar los ciberdelitos, la regulación para proveedores de servicios de Internet también requiere complementarse para que éstos mantengan el registro de actividad en su plataforma y aporten información ante un posible incidente. Por otra parte, se requiere establecer acuerdos internos y crear convenios de cooperación con otros países para la atención del cibercrimen y el ciberterrorismo que atentan contra la seguridad nacional.	Regulación de algunos ciberdelitos en las siguientes leyes: Código Penal Federal, Código Penal del Distrito Federal, Código Federal de Procedimientos Penales, Ley de Protección de Datos de Colima, y Códigos Penales de los Estados de Aguascalientes, Sinaloa, Tabasco y Tamaulipas; El 30 de abril de 2009 se publicó en el Diario Oficial de la Federación el Decreto por el que se adiciona la fracción XXIX-O del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, la cual establece la facultad del Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares; El 1 de junio de 2009 se publicó el decreto por el que se adiciona al artículo 16 de la Constitución un segundo párrafo, reconociendo que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros; Se cuenta con el Equipo de Respuesta a Incidentes de Seguridad en cómputo de la Universidad Nacional Autónoma de México que atiende problemas de seguridad en el ámbito	Crear legislaciones adecuadas o actualizar las existentes en caso necesario para la protección de la información en el ciberespacio; Capacitación a los jueces en temas de ciberseguridad con el fin de que puedan entender la naturaleza de los ciberdelitos y dar sentencias acordes a los mismos; Creación de CSIRT nacionales para coordinar los esfuerzos de atención ante incidentes de seguridad mayores y para que sean los puntos de contacto con otros países; Mantener una comunicación permanente entre CSIRT nacionales con el fin de coordinarse en caso de un incidente regional o mundial; Realización de foros de intercambio de experiencias y de capacitación para los equipos de seguridad miembros de la comunidad internacional; Realización de convenios internacionales de colaboración en contra de los ciberdelitos con el fin de agilizar las investigaciones y formar un frente común.

[377] Informe del Secretario General A/65/154, Naciones Unidas: Asamblea General. 20 de julio de 2010.

	académico y brinda apoyo y asesoría técnica a las autoridades de gobierno en México para la atención de delitos cibernéticos; Se tiene una Policía Cibernética dentro de la Policía Federal para dar seguimiento a las investigaciones sobre delitos de seguridad pública; Se está generando dentro del Gobierno Federal un informe ejecutivo en materia de vulnerabilidad cibernética para informar a las altas autoridades del gobierno federal sobre los incidentes cibernéticos a nivel mundial con el fin de prever y apoyar iniciativas que contribuyan a fortalecer la ciberseguridad en México; Se está planeando dentro del Gobierno Federal la creación de un CSIRT nacional con el fin de coordinar los esfuerzos de atención de los ciberdelitos a nivel interno y externo; Se realizan programas de concientización del público en general, coordinadas por entidades públicas y privadas para prevenir los delitos cibernéticos; Se asiste a diferentes foros y se establecen acuerdos de buena voluntad con otros países para la atención de ciberdelitos.	

FUENTES CONSULTADAS

Bibliografía

Arreola, Adolfo. *Ciberespionaje: la puerta al mundo virtual de los estados e individuos: una revisión de los programas de espionaje digital de Estados Unidos*. Siglo XXI Editores, México, 2015.

Astié, Walter y Rosas María. *Las relaciones internacionales en el siglo XXI*. Universidad Nacional Autónoma de México, México, 2017.

Borja, Jordi y Castells, Manuel. *Local y Global. La gestión de las ciudades en la era de la información*. Taurus, España, 1997.

Buzan, Barry. *People, States & Fear, an Agenda for International Security Studies in the Post-Cold War Era*. Harvester Wheatsheaf, London, 1991.

Buzan, Barry y Weaver Ole. *Regions and Powers. The Structure of International Security*. Cambridge University Press, New York, 2004.

Cintra, José T. *Seguridad Nacional, Poder Nacional y Desarrollo*. CISEN, México, 1997.

Castells, Manuel. *La Era de la Información Económica, Sociedad y Cultura. La sociedad Red*. Alianza, Madrid, 1998.

Curzio, Leonardo. *La seguridad nacional de México y la relación con Estados Unidos*. Universidad Nacional Autónoma de México, México, 2007.

Held, David. *Transformaciones globales. Política, economía y cultura*. Oxford University Press, México, 2002.

Garduño Valero, Guillermo. "Metodología de la estrategia y la seguridad nacional". En la seguridad nacional de México. Debate actual, coordinado por José Luis Piñeyro, México, 2003, pp. 69-106.

Jordan, Amos y Taylor William. *American National Security, Policy and Process*, Hopkins University Press, London, 1984.

Kaldor, Mary. *El poder y la fuerza. La seguridad de la población civil en un mundo global*, Tusquets Editores México, México, 2011.

Keohane, Robert y Nye, Joseph. *Poder e interdependencia*. GEL, Buenos Aires, 1988.

Landes, D.S. *Proceso tecnológico y revolución industrial*. Tecnos, Madrid, 1979.

Mele, Stefano. "La batalla por el ciberespacio y el ciberarmamento". *Vanguardia Dossier*. N. 54, 2015, pp. 38-41.

Muñoz, Alejandra. "La corrupción como amenaza a la seguridad nacional tras la transición democrática en México". Tesis de licenciatura, Universidad de las Américas Puebla, 2005.

Naím, Móises. *El Fin del Poder*. Debate, México, 2015.

Ortega, Adriana y Gónzalez, Misael. “Transnacionalismo”, en Teorías de Relaciones Internacionales en el siglo XXI, editado por Jorge Schiavon *et al*. Asociación Mexicana de Estudios Internacionales, A.C. México, 2016.

Piñeyro, José Luis. *La seguridad nacional en México. Debate actual*. Universidad Autónoma Metropolitana-Azcapotzalco, México, 2005.

Sánchez Belmont, Óscar. *Inteligencia y contrainteligencia*. Ediciones Gernika, México, 2014.

Von Clausewitz, Carl. *On War*, Princeton University Press, Nueva Jersey, 1984.

Waltz, Kenneth. *El hombre, el Estado y la guerra. Un análisis teórico*. Centro de Investigación y Docencia Económicas, México, 2013.

Documentos en PDF

“Actualidades de la UIT”. *Unión Internacional de Telecomunicaciones*. 2010, http://bit.ly/2m8ukgB

Aguirre, Arsenio. “Ciberseguridad en Infraestructuras Críticas de Información”. Tesis de maestría, Universidad de Buenos Aires, 2017, http://bit.ly/2kFKyxg

Aguirre, Joao. “Inteligencia estratégica: un sistema para gestionar la innovación”. *Universidad ICESI*, Estudios Gerenciales, Vol. 31, 2015, pp. 100-110, http://bit.ly/2lOU2GF

“Amenazas Cibernéticas al sector financiero mexicano”. *Control Risks*, 2015 http://bit.ly/2lK4a3A

Andrew Lewis, James. “Experiencias avanzadas en políticas y prácticas de ciberseguridad”. *Banco Interamericano de Desarrollo*, 2016, http://bit.ly/2lNFG9y

Arbeláez, Ángela. “La Noción de Seguridad en Thomas Hobbes”. *Revista Facultad de Derecho y Ciencias Políticas*. Vol. 39, n.° 110, 2009, pp. 97-124, http://bit.ly/2lPcn6s

Bandala, Marco. “Reconceptualización de la Seguridad Nacional: una aproximación para México”. *ININVESTAM*. Documento de análisis DA. 24/18, 2018, http://bit.ly/2kfn1TU

Benítez Manaut, Raúl. “La seguridad nacional en la indefinida transición: mitos y realidades del sexenio de Vicente Fox”. *Revista Foro Internacional*, (191-192), 2008, pp. 184-208, http://bit.ly/2kefpRy

Benítez Manaut, Raúl en Marcos Pablo Moloeznik. “Tratado sobre pensamiento estratégico-militar (Enseñanzas para el Sistema de Defensa de México)”. *CASEDE*, 2018, pp. ix-xiv, http://bit.ly/2mbjwOU

Candau, Javier. “Estrategias nacionales de ciberseguridad. Ciberterrorismo”. En Cuadernos de Estrategia 149, 2010, pp. 259-322, http://bit.ly/2mb0x77

Carlini, Agnese. “Ciberseguridad: un nuevo desafío para la comunidad internacional”. *Instituto Español de Estudios Estratégicos*, Documento de opinión, 2016, http://bit.ly/2m3f7xg

Castrillón-Riascos, Javier. “Nada volverá a ser igual: ciberguerra y ciberpoder”. *Memorias*. Vol. 13, n. 23, 2015, pp. 115-127, http://bit.ly/2mbZrbh

Chaves, Julián. “Desarrollo Tecnológico en la Primera Revolución Industrial”. *Norba. Revista de Historia*, N° 17, 2004, pp. 93-109, http://bit.ly/2kD5BAJ

Comisión Europea. “Agenda Digital para Europa”. *Unión Europea*. 2014, http://bit.ly/2mbboOo

“Cuarto Informe de Gobierno”. *Presidencia de la República*, 2016, http://bit.ly/2lL58N1

Cujabante, Ximena. “La seguridad internacional: evolución de un concepto”. *Revista de Relaciones Internacionales, Estrategia y Seguridad*. Vol. 4 n.° 2, 2009, pp. 93-106, http://bit.ly/2lHqkUi

“Declaración sobre seguridad en las Américas”. *Organización de los Estados Americanos*, 2003, http://bit.ly/2kfVEZW

De Miguel, Jesús. “Unas reflexiones sobre la seguridad internacional en el siglo XXI”. *ININVESTAM*. Documento de Análisis, DA. 06/16, 2016, http://bit.ly/2lHLjX2

----------. “Reflexiones sobre la ley de seguridad nacional”, ININVESTAM, Documento de Opinión, DO. 11/16, México, 2016, http://bit.ly/2lHirhF

----------. “Construyendo una estrategia de seguridad nacional para México”. *ININVESTAM*. Documento de Análisis, DA. 25/16, 2016, http://bit.ly/2k6nZ4C

----------. “La Seguridad Nacional y la gran estrategia”. *ININVESTAM*, Documento de Análisis, DA. 50/18, 2018, http://bit.ly/2mc6qkB

Demurtas, Alessandro. “El complejo europeo de seguridad regional entre 2001 y 2011 a las amenazas del terrorismo islamista y de las armas de destrucción masiva”. Tesis doctoral, Universitat Autònoma de Barcelona, 2014, http://bit.ly/2kDWjo4

Enríquez, Carlos. “Estrategias internacionales para el ciberespacio”. En Monografías del CESEDEN 126, 2012, pp. 71-116, http://bit.ly/2m3RGUz

“Estrategia de Ciberseguridad del Banco de México”. *Banco de México*, 2018, http://bit.ly/2ktwerX

“Estrategia de ciberseguridad nacional”. *Gobierno de España. Presidencia del Gobierno*. 2013, http://bit.ly/2m3Qvo7

“Estrategia Nacional de Ciberseguridad”. *gob.mx*, 2017, http://bit.ly/2ktuizH

Evans, Dave. “Internet de las Cosas. Cómo la próxima evolución de Internet lo cambia todo”. *CISCO*, 2011, pp. 1-12, http://bit.ly/2kfRRvG

Feliu, Luis. “La ciberseguridad y defensa”. En Monografías del CESEDEN 126, 2012, pp. 35-70, http://bit.ly/2m3RGUz

Fernández, Rafael (coord.). “Perspectiva de ciberseguridad en México”. *McKinsey&Company y COMEXI*, Documento colaborativo, 2018, http://bit.ly/2kfSZPW

Gaudiano, Paolo. “Qué entendemos por «cosas» en el Internet de las cosas”, *Fundación de la Innovación Bankiter*. 2011, pp. 11-20, http://bit.ly/2ma96iy

Ganuza, Néstor. “La situación de la ciberseguridad en el ámbito internacional y en la OTAN”. En Cuadernos de Estrategia 149, 2010, pp. 167-214, http://bit.ly/2mb0x77

“Global Cybersecurity Index 2017”. *International Telecommunication Union*, 2017, http://bit.ly/2kD8GRj

“Global Cybersecurity Index 2018”. *International Telecommunication Union*, 2019, http://bit.ly/2lHoMts

González, Abraham. “El ciberespacio en la guerra moderna”. *ININVESTAM*. Documento de Análisis, DA. 21/18, 2018, http://bit.ly/2keaoII

González, Guadalupe. “Una perspectiva global para la Seguridad Nacional de México”. *Revista de Administración Pública*. Vol. L, n. 1, 2015, pp. 267-290, http://bit.ly/2lKeDMB

“Guía de ciberseguridad para los países en desarrollo”. *Unión Internacional de Telecomunicaciones*, 2007, http://bit.ly/2lKfq01

“Informe de Avance y Resultados 2018”. *Secretaría de la Defensa Nacional*, 2018, http://bit.ly/2lG9UeJ

“Informe de Avance y Resultados 2018”. *Secretaría de Marina*, 2018, http://bit.ly/2lNL3pe

J. Verdes-Montenegro, Francisco. “Securitización: agendas de investigación abiertas para el estudio de la seguridad”. *Relaciones Internacionales*. N.° 29, 2015, pp. 111-131, http://bit.ly/2kfndm6

“La Protección de Infraestructura Críticas y la Ciberseguridad Industrial”. *Centro de Ciberseguridad Industrial*, 2013, http://bit.ly/2mbiF0E

“Ley Orgánica de la Armada de México”. *Cámara de Diputados del H. Congreso de la Unión*, http://bit.ly/2lHAyEa

“Ley Orgánica del Ejército y Fuerza Aérea Mexicanos“. *Cámara de Diputados de H. Congreso de la Unión*, http://bit.ly/2kedpJ5

“Ley de la Policía Federal”. *Cámara de Diputados del H. Congreso de la Unión*, http://bit.ly/2ktGdNU

“Ley de Seguridad Nacional”. *Cámara de Diputados del H. Congreso de la Unión*, http://bit.ly/2kaR7I1

Llorens, María Pilar. “Los desafíos del uso de la fuerza en el ciberespacio”. *Anuario Mexicano de Derecho Internacional*. Vol. XVII, 2017, pp. 785-816, http://bit.ly/2kDbNst

López, Javier. “La evolución del conflicto hacia un nuevo escenario bélico”. En Monografías del CESEDEN 126, 2012, pp. 117-166, http://bit.ly/2m3RGUz

Machín, Nieva y Gazapo Manuel. “La ciberseguridad como factor crítico en la seguridad de la Unión Europea”. *Revista UNISCI*. N.°42, 2016, pp. 47-68, http://bit.ly/2kfTN7q

Martínez, Clara. “El uso de ciberataques como herramienta de relaciones internacionales por parte de actores estatales: los casos de Estados Unidos y Rusia”. Trabajo de fin de grado, Universidad Pontificia Comillas ICAI-ICADE, 2015, http://bit.ly/2m3Q6C7

Ministerio de la Presidencia. “Informe Anual de Seguridad Nacional 2015”. *Departamento de Seguridad Nacional*, 2016, España, http://bit.ly/2lNVtoQ

Moliner, Juan. “La Cumbre de la OTAN en Varsovia”. *Instituto Español de Estudios Estratégicos*. Opinión 79bis/2016, 2016, http://bit.ly/2kD9WE1

Orozco, Gabriel. “El aporte de la Escuela de Copenhague a los estudios de seguridad”. *Revista Fuerzas Armadas y Sociedad*. N.° 1, 2006, pp. 141-162, http://bit.ly/2lKeUz7

Otálvaro, Andrés. “La seguridad internacional a la luz de las estructuras dinámicas regionales: una propuesta teórica de complejos de seguridad regional”. *Desafíos*, 2004, pp. 22-242, http://bit.ly/2lOTf8F

Piana, Ricardo y Cruz Juan. “Globalización, interdependencia compleja y mundialización: la dialéctica entre lo global y lo local”, *Razón Crítica*. 3, 2017, pp. 145-173, http://bit.ly/2ma7Agm

Piñeyro, José Luis y Gabriela Barajas. “La seguridad nacional con Fox: avances analíticos, retrocesos reales”. *Revista Foro Internacional*, (191-192), 2008, p. 209-237, http://bit.ly/2keeror

“Plan Nacional de Desarrollo 2013-2018”. *Gobierno de la República*, 2013, http://bit.ly/2ktKd0U

“Plan Nacional de Desarrollo 2019-2024”. *Presidencia de la República*, 2019, http://bit.ly/2lPlwMk

“Primer Informe de Gobierno”. *Presidencia de la República*, 2013, http://bit.ly/2lGch17

“Programa para la Seguridad Nacional 2014-2018”. *Presidencia de la República*, 2014, http://bit.ly/2lK44ce

“Programa Sectorial de Defensa Nacional 2013-2018”. *Secretaría de la Defensa Nacional*, 2013, http://bit.ly/2lHfLR9

“Programa Sectorial de Marina 2013-2018”. Secretaría de Marina, http://bit.ly/2kakdqX

“Puntos importantes sobre la situación actual del SPEI”. Banco de México, 22 de mayo de 2018, http://bit.ly/2m3crjc

“Quinto Informe de Gobierno”. *Presidencia de la República*, 2017, http://bit.ly/2lL5a7B

“Recomendaciones para el Desarrollo de la Estrategia Nacional de Ciberseguridad”. *Organización de los Estados Americanos*, 2017, http://bit.ly/2lHV5Ze

Rego, Miguel. “Un llamado a la acción para proteger a ciudadanos, sector privado y Gobierno”. *Organización de los Estados Americanos*, 2018, http://bit.ly/2lPQ0hh

Reyes, Giovanni. “Teoría de la Globalización: Bases fundamentales”. *Revista de la Facultad de Ciencias Económicas y Administrativas*. Vol. 2, n.° 1, 2001, pp. 43-53, http://bit.ly/2kD58OZ

Ruiz, Joaquín. “Ciberamenazas: ¿el terrorismo del futuro?”. *Instituto Español de Estudios Estratégicos*. Documento de Opinión, 19 de agosto de 2016, http://bit.ly/2kaclFV

Sain, Gustavo. “¿Qué es la ciberguerra?”. *Revista Pensamiento Penal*. S.f., http://bit.ly/2kFBdFL

Salas, Edmundo. “Reflexiones en torno a la Seguridad Nacional y la Seguridad Interior”. *Revista de Administración Pública*. Volumen L, n.° 1, México, 2015, 291-317, http://bit.ly/2lKeDMB

Sánchez, Gema. “Los Estados y la Ciberguerra”. *Ministerio de Defensa: Centro Superior de Estudios de la Defensa Nacional*. N.° 317, 2010, p.63-76, http://bit.ly/2lIXC5i

----------. “La ciberguerra: los casos de Stuxnet y Anonymous”. *DERECOM*. N. 11, 2012, pp. 124-133, http://bit.ly/2kDaeKY

----------. “El ciberespionaje”. *DERECOM*. N. ° 13, 2013, pp. 115-124, http://bit.ly/2ke5DPp

“Segundo Informe de Gobierno”. *Presidencia de la República*, 2014, http://bit.ly/2k8X7kw

“Sexto Informe de Gobierno”. *Presidencia de la Repúbica*, 2018, http://bit.ly/2lL5fbp

“Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization”. *NATO*. Summit in Lisbon, 2010, http://bit.ly/2kafjKz

“Tendencias de Seguridad Cibernética en América Latina y el Caribe 2014”. *Organización de los Estados Americanos/Symantec*, 2014, https://symc.ly/2lKmdXz

“Tercer Informe de Gobierno”. *Presidencia de la República*, 2015, http://bit.ly/2lGcv8t

Trujillo, Patricia. “El ciberespacio, recurso y responsabilidad de los Estados”. *ININVESTAM*, México, 2017, http://bit.ly/2m5hyPT

Vizarretea Rosales, Emilio. “Nueva inteligencia y ciberseguridad”. *Revista del Centro de Estudios Navales*. Vol. 37, 2016, pp. 49-82, http://bit.ly/2lNMm7C

Páginas de Internet

“Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA)”. *Unión Europea*, s.f., http://bit.ly/2lH9cht

“Amenazas y Riesgos”. *Centro de Investigación y Seguridad Nacional*, s.f., http://bit.ly/2lPMdAz

“Artículo 26”. *Orden Jurídico*, http://bit.ly/2kalvCj

“Artículo 89 constitucional”. *Orden Jurídico*, http://bit.ly/2m5lBM5

“A un año de WannaCry el exploit EternalBlue sigue siendo un vector de infección”. *Kaspersky Lab*, 11 de mayo de 2018, http://bit.ly/2kDdeHn

“Big Data: ¿En qué consiste? Su importancia, desafíos y gobernabilidad”. *PowerData*, s.f., http://bit.ly/2lIZbQI

“Centre is the first International Military Organization hosted by Estonia”. *NATO Cooperative Cyber Defence Centre of Excellence*, s.f., http://bit.ly/2ktA1Wa

“Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal”. *Policía Federal*, 17 de mayo de 2018, http://bit.ly/2kecNDh

“Ciberespacio”. *Real Academia Española*, s.f., http://bit.ly/2ma0OXV

“CNS fortalece capacidades del sistema de protección física para infraestructuras vitales”. *Servicio de Protección Federal*, 08 de febrero de 2018, http://bit.ly/2lPNCXR

“Cómo actualizar Windows para reparar la vulnerabilidad EternalBlue y evitar el ataque DoublePulsar”, AVG, s.f., http://bit.ly/2kfXOJ2

“Coordinación de Seguridad de la Información UNAM-CERT”. *Universidad Nacional Autónoma de México*, s.f., http://bit.ly/2kDfo9X

“Cyber Definitions”. *NATO Cooperative Cyber Defence Centre of Excellence*, s.f., http://bit.ly/2lPcZsM

“Decisiones destacadas en Guadalajara”. *Unión Internacional de Telecomunicaciones*, noviembre de 2010, http://bit.ly/2kFUVkH

“De qué manera distinguir el cibercrimen y protegerse”. *Norton by Symantec*, s.f., https://nr.tn/2lHJwkM

“Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética”. *Organización de los Estados Americanos*, 10 de junio de 2003, http://bit.ly/2lOVR6t

“Día de la independencia”. *Embajada de Estonia en Madrid*, s.f., http://bit.ly/2kfqhi6

“Digital Single Market”. *European Commission*, s.f., http://bit.ly/2kaebXl

“División Científica”. *Policía Federal*, s.f., http://bit.ly/2ktHswA

“Estados Miembros”. *NATO/OTAN*, s.f., http://bit.ly/2kFCTz3

“Estados Miembros”. *Organización de los Estados Americanos*, s.f., http://bit.ly/2k6qALU

“Foro de Ciberseguridad”. *Comisión Nacional Bancaria y de Valores*, 23 de octubre de 2017, http://bit.ly/2lHBqbU

“History”. *NATO Cooperative Cyber Defence Centre of Excellence*, s.f., http://bit.ly/2lJXxye

Gastón, Lucía. “Qué es la Directiva NIS”. *BBVA*, 26 de marzo de 2018, https://bbva.info/2m3RKnh

Gobierno de España. “¿Qué es la Alianza Atlántica, qué es la OTAN?”. *Ministerio de Asuntos Exteriores y de Cooperación*, 20 de abril de 2015, http://bit.ly/2mbbIN6

“Índice Global de Ciberseguridad 2017”. *Foro Jurídico*, 5 de julio de 2018, http://bit.ly/2kFW8Zh

“Industrial”. *Real Academia Española*, s.f., http://bit.ly/2kv0H91

“Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional”. *Naciones Unidas. Asamblea General*. A/65/201, http://bit.ly/2mbXrzT

----------. *Naciones Unidas. Asamblea General*, A/68/98, http://bit.ly/2ktACXW

----------. *Naciones Unidas. Asamblea General*. A/70/174, http://bit.ly/2lHrVcK

“Informe del Secretario General”. *Naciones Unidas. Asamblea General*. A/65/154, http://bit.ly/2lJ1KCk

Infosecurity. “Japón desarrollará una agencia de élite de sombreros blancos”. *UNAM-CERT*, 20 de mayo de 2016, http://bit.ly/2kDmkDZ

“Interoperability services: x-road”. *e-estonia*, s.f., http://bit.ly/2ktCwrw

“Introducción”. *UNODA*, s.f., http://bit.ly/2kfTycw

“ISO / IEC 27001: 2013”. *Organización Internacional de Normalización*, s.f., http://bit.ly/2kFJ9qx

“Ley de Planeación”. *Cámara de Diputados del H. Congreso de la Unión*, http://bit.ly/2lK4W0u

“Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional”. *Naciones Unidas. Asamblea General*. A/RES/53/70, http://bit.ly/2kad1uX

“Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional”. *UNODA*, http://bit.ly/2lHrHSW

“México”. *Organización de los Estados Americanos*, s.f., http://bit.ly/2mb0Ui1

“MéxicoDigital”, s.f., http://bit.ly/2kb9xsa

“Nació filósofo Thomas Hobbes”. *History*, s.f., http://bit.ly/2ke4JlZ

“NATO Organization”. *North Atlantic Treaty Organization NATO/OTAN*, s.f., http://bit.ly/2mbYOyx

“Nuestro Propósito”. *Organización de los Estados Americanos*, s.f., http://bit.ly/2ke7CmP

“Nuevas Medidas para reforzar la ciberseguridad en Europa”. *Centro Criptológico Nacional*, 21 de septiembre de 2017, http://bit.ly/2lH9mW7

“Países”. *Unión Europea*, s.f., http://bit.ly/2lJ2Iys

“Plan de ciberseguridad de la UE para proteger una red abierta plena de libertad y de oportunidades en línea”. *Comisión Europea*, 07 de febrero de 2013, http://bit.ly/2lPGf2D

“¿Qué es bitcoin?”. *Bitcoin*, s.f., http://bit.ly/2lNjVqI

“¿Qué es Fintech?”. *FinTech México*, s.f., http://bit.ly/2kb6KPP

“¿Qué es el CISEN?”, Centro de Investigación y Seguridad Nacional, s.f., http://bit.ly/2lPMbsr

“¿Qué es el Convenio de Budapest?”. *NIC Argentina*, diciembre 2017, http://bit.ly/2kb8yIB

“¿Qué es la Cuarta Revolución Industrial?”. *Salesforce Latinoamérica*, https://sforce.co/2lHp9Em

“¿Qué es la Estrategia Digital Nacional?”. *Presidencia de la República*, 17 de mayo de 2014, http://bit.ly/2lNkSzi

“¿Qué es MAAGTICSI?”. *Secretaría de Desarrollo Agrario, Territorial y Urbano*, s.f., http://bit.ly/2kr48NX

“¿Qué es un Ransomware?”. *Panda Security*, 15 de noviembre de 2013, http://bit.ly/2lK13Zs

"¿Qué hace la UIT?". *Unión Internacional de Telecomunicaciones*, s.f., http://bit.ly/2mbXqfd

"Quiénes somos". *Organización de los Estados Americanos*, s.f., http://bit.ly/2lNEdA4

"Ransomware: definición, prevención y eliminación". *Kaspersky Lab*, s.f., http://bit.ly/2m39xei

"Resolución aprobada por la Asamblea General el 2 de diciembre de 2011". *Naciones Unidas. Asamblea General*. A/RES/66/24, http://bit.ly/2kb0PtY

"Revolución". *Real Academia Española*, s.f., http://bit.ly/2mb8ol6

Selva, Vicent. "Revolución Industrial IV". *Economipedia*, s.f., http://bit.ly/2m3OWqf

"Secretaría de Seguridad Multidimensional". *Organización de Estados Americanos*, s.f., http://bit.ly/2ktAyHE

"Seguridad". *Real Academia Española*, s.f., http://bit.ly/2kD4YXK

"Seguridad Cibernética". *Organización de los Estados Americanos*, s.f., http://bit.ly/2kDar0R

"Seguridad colectiva". *Ministerio de Asuntos Exteriores y Cooperación*, 20 de abril de 2015, http://bit.ly/2ke7aoD

"Virus y gusanos informáticos". *Kaspersky Lab*, s.f., http://bit.ly/2lNGN9e

"Visión General". *Unión Internacional de Telecomunicaciones*, http://bit.ly/2kaJbqd

Mesografía

"10 puntos para entender la nueva ley fintech". *El Financiero*, 01 de marzo de 2018, http://bit.ly/2kb7vbw

Albors, Josep. "¿Sabes qué es un exploit y cómo funciona?". *Welivesecurity*, 09 de octubre de 2014, http://bit.ly/2kGmjiH

Álvarez, Carmen. "México, más vulnerable a ciberataques". *Excélsior*, 26 de agosto de 2016, http://bit.ly/2ktG9xG

Arreola, Javier. "Ciberseguridad (casi) a prueba del enemigo 'invisible'". *Forbes México*, 20 de mayo de 2016, http://bit.ly/2ma7WUb

Arteaga, Félix. "La dimensión internacional de la ciberseguridad". *Real Instituto Elcano Royal Institute*, 24 de julio de 2018, http://bit.ly/2kFWMWG

Balbi, Muriel. "Los 7 secretos del país más digital del mundo". *Infobae*, 25 de noviembre de 2017, http://bit.ly/2m38tqO

"Banxico crea oficina de ciberseguridad tras hackeo a bancos". *Forbes México*, 15 de mayo de 2018, http://bit.ly/2kFV33E

Barranco, Ricardo. “¿Qué es Big Data?”. *IBM developWorks*, 18 de junio de 2018, https://ibm.co/2kGgzFF

Blanco, Daniel. “A esta velocidad corre el cronómetro de pérdidas económicas por el ciberataque global”. *El Financiero*, 14 de mayo de 2017, http://bit.ly/2kGIIxt

Chávez, Gabriela. “El cibercrimen le cuesta 107 mdd a la banca mexicana: OEA”. *Expansión*, 11 de julio de 2019, http://bit.ly/2kE7X2g

“El ciberataque de escala mundial y ‘dimensión nunca antes vista’ que afectó a instituciones y empresas de unos 15 países”. *BBC Mundo*, 13 de mayo de 2017, https://bbc.in/2keaMa8

“El nuevo campo de entrenamiento para las ciberguerras”. *BBC Mundo*, 18 de junio de 2011, http://bit.ly/2ktD4h6

“El virus que tomó control de mil máquinas y les ordenó autodestruirse”. *BBC Mundo,* 11 de octubre de 2015, https://bbc.in/2m39jns

Espino, Manuel. “PGR tiene distintas líneas de investigación sobre ataque cibernético”. *El Universal*, 16 de mayo de 2018, http://bit.ly/2ktv4wB

Fernández, Álvaro. “Estonia, baluarte de la ciberseguridad europea”. *El Orden Mundial*, 12 de agosto de 2015, http://bit.ly/2lJ4D68

Fisher, Dennis. “Qué es un botnet?”. *Kaspersky Lab*, 25 de abril de 2013, http://bit.ly/2ktBVpM

Fonseca, Cristina. “¿Cómo capacitarnos para la Cuarta Revolución Industrial?”, *World Economic Forum*, 16 de enero de 2017, http://bit.ly/2kDVrzO

Gray, Alex. “Estos son los mayores riesgos que enfrenta el mundo”. *World Economic Forum*, 17 de enero de 2018, http://bit.ly/2kaOVQN

Gutiérrez, Fernando. “CNBV: endurecer reglas en ciberseguridad del sistema financiero mexicano”. *El Economista*, 22 de agosto de 2018, http://bit.ly/2m8DKst

Lara, Paul. “Estados Unidos hackeó a Segob, Sedesol y UNAM”. *Imagen Digital*, 01 de noviembre de 2016, http://bit.ly/2kfZlPi

La Razón Online. “Vulnerables a hackeo 6 de cada 10 firmas”. *La Razón de México*, 26 de marzo de 2019, http://bit.ly/2kaVAup

Lipovsky, Robert. “A siete años de Stuxnet, los sistemas industriales están nuevamente en la mira”. *Welivesecurity by eset*, 20 de junio de 2017, http://bit.ly/2lPJqaz

Márquez, William. “Ciberespacio: el nuevo ámbito de la guerra para el Pentágono”. *BBC Mundo*, 27 de julio de 2011, https://bbc.in/2lHOM80

Martínez, Francisco. “La vida después de wannacry”. *Dirección General de Cómputo y de Tecnologías de Información y Comunicación*. UNAM, s.f., http://bit.ly/2m6sMDO

Martínez, Ricardo. “Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE”. *El País*, 18 de mayo de 2007, http://bit.ly/2lKj3TH

McGuiness, Damien. “Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país”. *BBC Mundo*, 06 de mayo de 2017, https://bbc.in/2ktrG4R

Mendoza, Miguel. “NIS: ¿qué es y qué implica esta nueva legislación en seguridad?”. *Welivesecurity by eset*, 22 de julio de 2016, http://bit.ly/2ktzrrs

Meschoulam, Mauricio. “Ciberguerra en 2016: las armas de disrupción masiva”. *El Universal*, 24 de octubre de 2016, http://bit.ly/2lNz4YM

“México: el ciberataque “sin precedentes” a los bancos del país que causó pérdidas millonarias”. *BBC Mundo*, 15 de mayo de 2018, https://bbc.in/2kajgyT

Miguel Gil, Javier. “La integración del ciberespacio en el ámbito militar”. *Universidad de Granada*, 11 de octubre de 2017, http://bit.ly/2k8PF92

Myers, Lisa. “Security terms explained: What does Zero Day mean?”. *Welivesecurity by eset*, 11 de febrero de 2015, http://bit.ly/2kqZqQh

Nava, Diana. “¿Qué retos tiene México ante un ciberataque?”. *El Financiero*, 19 de mayo de 2017, http://bit.ly/2kDdZjH

Ortega, Omar. “¿Qué tan protegido está México ante la ciberdelincuencia?”. *El Financiero*, 30 de mayo de 2017, http://bit.ly/2kE3L2w

Ortega, Omar. “México, la tercera nación con más ciberataques en el mundo”. *El Financiero*, 30 de julio de 2018, http://bit.ly/2mbhzC4

Perasso, Valeria. “Qué es la Cuarta Revolución Industrial (y por qué debería preocuparnos)”. *BBC Mundo*, 12 de octubre de 2016, https://bbc.in/2kFU4jZ

Pérez, Jenny. “Europa y la guerra por el ciberespacio”. *Deutsche Welle*, 16 de febrero de 2018, http://bit.ly/2mad0Ie

“¿Qué es el SPEI?”. *El Economista*, 03 de mayo de 2018, http://bit.ly/2kDfiyY

Riquelme, Rodrigo. “Ataques cibernéticos a la cadena de suministro aumentan 78% en un año”. *El Economista*, 04 de marzo de 2019, http://bit.ly/2m8GciF

Riquelme, Rodrigo. “Marco jurídico, reto del próximo gobierno en ciberseguridad”. *El Economista*, 02 de agosto de 2018, http://bit.ly/2keh5uk

Riquelme, Rodrigo. “México cae 35 lugares en Índice Global de Ciberseguridad de la ITU”. *El Economista*, 06 de mayo de 2019, http://bit.ly/2ma6VeS

Rosas, María Cristina. “Ciberespacio, crimen organizado y seguridad nacional”. *América Latina en movimiento*, 08 de mayo de 2011, http://bit.ly/2lJZ4Eu

Rouse, Margaret. “Ataque de Denegación de Servicio (DDoS)”. *TechTarget*, s.f., http://bit.ly/2mb1yvX

Sánchez, Julio. “Política de ciberseguridad en México tiene un camino sinuoso”. *El Economista*, 27 de diciembre de 2016, http://bit.ly/2kfuSkm

Sánchez, Julio. “Colaboración y divulgación, desafíos de la ciberseguridad en México”. *El Economista*, 17 de agosto de 2017, http://bit.ly/2lL618j

Shakeel, Bhat. “DoublePulsar-A very sophisticated Payload for Windows”. *Secpod*, 01 de junio de 2017, http://bit.ly/2lK1OSi

Sharp, Andy y Tweed David. “Estados Unidos culpa a Norcorea por ataque ‘cobarde’ de WannaCry”. *El Financiero*, 19 de diciembre de 2017, http://bit.ly/2mc2RLf

Telcel. “Internet de las Cosas”. *Forbes México*, 18 de diciembre de 2014, http://bit.ly/2lNAFxK

Tejado, Javier. “México reprobado en ciberseguridad”. *El Universal*, 28 de julio de 2015, http://bit.ly/2lL2iaP

Terradas, Nicolás. “El dilema de seguridad y su importancia para el estudio de las relaciones internacionales”. *Revista Letras Internacionales*, n.° 88-3, 2009, http://bit.ly/2lPckYk

Tidy, Joe. “Me odian y me persiguen por destruir virus en internet”. *BBC Mundo*, 19 de marzo de 2019, https://bbc.in/2kD3soF

Tomás, Aurelio. “La seguridad tiene cinco dominios: aire, tierra, mar, espacio y ciberespacio”. *PERFIL*, 07 de julio de 2018, http://bit.ly/2kDTiUM

Valadés, Bernardo. “Entrevista”. *Segurilatam*, 1 de marzo de 2016, http://bit.ly/2kcM1Lo

Ventura, Daniel. “Ciberguerra: la lucha de las grandes potencias por controlar internet”. *Huffpost Español*, 07 de febrero de 2017, http://bit.ly/2kDaOIN